Don Springmeyer, Esq. (#1021)
Michael J. Gayan, Esq. (#11135)
Kemp Jones, LLP
3800 Howard Hughes Parkway, 17th Floor
Las Vegas, Nevada 89169
P: (702) 385-6000
d.springmeyer@kempjones.com
Liaison Counsel

John A. Yanchunis
Morgan & Morgan
Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
P: (813) 223-5505
jyanchunis@ForThePeople.com
Interim Class Counsel

Douglas J. McNamara
Cohen Milstein Sellers & Toll PLLC
1100 New York Ave. NW
5th Floor
Washington, D.C. 20005
P: (202) 408-4600
dmcnamara@cohenmilstein.com
Interim Class Counsel

Amy E. Keller
DiCello Levitt LLP
10 North Dearborn Street
Sixth Floor
Chicago, Illinois 60602
Tel. (312) 214-7900
akeller@dicellolevitt.com
Interim Class Counsel

Counsel for Plaintiffs and the Class

(Additional Counsel Listed on Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

In re: DATA BREACH SECURITY LITIGATION AGAINST CAESARS ENTERTAINMENT, INC.	**Case No. 2:23-cv-01447-ART-BNW** **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

TABLE OF CONTENTS

Plaintiffs Dhaman Gill, James Martin, April Elvidge, Monica Blair-Smith, Carey Hylton, Charles Popp, Crystal Brewster, Cynthia Rubner, David Lackey, Isaac Dwek, John Gedwill, Laura McNichols, Thomas McNichols, Mark Huddleston, Miguel Rodriguez, Todd Katz, Virginia Stacy, William Rubner, and Edward Cherveny ("Plaintiffs") bring this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class Members"), against Caesars Entertainment, Inc. ("Defendant" or "Caesars") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiffs.

I. INTRODUCTION

1. This is a class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a cyberattack on Caesars on or around August 23, 2023 (the "Data Breach"). Caesars has not disclosed the exact number of individuals impacted by the Data Breach, but it has confirmed that the cybercriminals were able to obtain a copy of Caesars' loyalty program database, including the driver's license numbers and Social Security numbers for a "significant number" of its more than 65 million program members.[1] Caesars' Form 8K disclosed that the breach even went beyond a copy of the loyalty program database, providing "[a]s a result of our investigation, on September 7, 2023, we determined that the unauthorized actor acquired a copy of, ***among other data***, our loyalty program database."[2] The Data Breach was directly caused by the Defendant's failure to adequately protect and secure the personally identifiable information ("PII") of its customers—in particular, members of its loyalty program—that it chose to collect

[1] Zack Whittaker, *Caesar's Entertainment says customer data stolen in cyberattack*, TechCrunch (Sept. 14, 2023), https://techcrunch.com/2023/09/14/caesars-entertainment-data-breach-cyberattack/; Caesars Entertainment, *Caesars Entertainment's Loyalty Program, Caesars Rewards®, Wins for "Best Customer Service" and "Best Promotion" at Prestigious Freddie Awards on April 21* (Apr. 22, 2022), https://investor.caesars.com/news-releases/news-release-details/caesars-entertainments-loyalty-program-caesars-rewardsr-wins. *See also* Caesars Entertainment, *Caesars Informational Website*, IDX (now removed), web.archive.org/web/20230914191948/https://response.idx.us/caesars/.

[2] *See* Caesars Entertainment, Inc. Form 8-K, Report of unscheduled material events or corporate event, at 2 (Sept. 14, 2023), *available at* https://investor.caesars.com/static-files/0bc13ee5-34a9-402e-8e7a-824b9dba4e57.

and keep.

2. According to reporting, the cyberattack that led to the Data Breach was conducted by a cybercriminal organization known as Scattered Spider, which specializes in gaining access credentials to a target's data systems by impersonating people in the organization through convincing phone calls.[3] The Data Breach reportedly originated from a social engineering attack on the company's outside IT vendor, which allowed the hackers access to the loyalty program database.[4]

3. According to Caesars, it has one of the largest loyalty programs in the gaming industry, with over 65 million members.[5] Caesars has the "largest and most diversified collection of gaming destinations in the U.S." and considers itself a "global leader in gaming and hospitality."[6] Based on available information, and belief, the Caesars' Data Breach likely involves tens of millions of its customers' PII.

4. Caesars' Rewards program allows members to earn credits they can use on a variety of services offered by Caesars, including gambling, hotel reservations, dining, and shopping.[7] However, to participate in the program, Caesars requires users to consent to the

[3] Sara Morrison, *The chaotic and cinematic MGM casino hack, explained*, Vox (Oct. 6, 2023), https://www.vox.com/technology/2023/9/15/23875113/Caesars-hack-casino-vishing-cybersecurity-ransomware.

[4] *Casino giant Caesars Entertainment confirms data breach*, Reuters (Sept. 14, 2023), https://www.stltoday.com/news/local/business/casino-giant-caesars-entertainment-confirms-data-breach/article_899b3b88-530b-11ee-9ed2-6b827d6c3b22.html.

[5] Caesars Entertainment, *Caesars Entertainment's Loyalty Program, Caesars Rewards®, Wins for "Best Customer Service" and "Best Promotion" at Prestigious Freddie Awards on April 21* (Apr. 22, 2022), https://investor.caesars.com/news-releases/news-release-details/caesars-entertainments-loyalty-program-caesars-rewardsr-wins.

[6] Caesars Entertainment, *Caesars Company Snapshot*, https://newsroom.caesars.com/overview/default.aspx (accessed Sept. 28, 2023, unchanged in relevant part as of July 24, 2024).

[7] Caesars Entertainment, *Earn and Redeem with Caesars Rewards®*, https://www.caesars.com/myrewards/earn-and-redeem (accessed Sept. 27, 2023, unchanged in relevant part as of July 24, 2024).

"collection and use of Member personal information" in accordance with Caesars' privacy policy.[8]

5. In its privacy policy, Caesars informs its Rewards program members that it may collect a large range of sensitive PII including first and last name, address, phone number, email address, credit card number, Social Security number, driver license number, passport number, license plate number, geolocation information, Caesars Rewards number, date of birth, purchase information, gaming activity information, biometric information, health information, and other similar information.[9]

6. After gaining access to Caesars' systems, the hackers extracted the loyalty member database and demanded Caesars pay a $30 million ransom.[10] According to reports, Caesars agreed to pay roughly half of the ransom demand to the hackers.[11] Even if true, that payment has done little to protect the PII or mitigate the resulting harm of Plaintiffs and Class Members, many of whom have already experienced fraud or attempted fraud or received notification that the exact data Caesars collected and failed to protect has been found on the Dark Web. Indeed, Caesars, itself, acknowledged that, while it had taken steps to have the stolen data erased by the cybercriminals, it could not "guarantee" that that data was, in fact, erased or not shared before it

[8] Caesars Entertainment, *Caesars Rewards® Rules & Regulations*, https://www.caesars.com/myrewards/caesars-rewards-rules-regs (accessed Sept. 27, 2023, unchanged in relevant part as of July 24, 2024).

[9] Caesars Entertainment, U.S. Privacy Policy (July 1, 2023) ("2023 Privacy Policy"), *available at* https://web.archive.org/web/20230825011104/https://www.caesars.com/corporate/privacyhttps://www.caesars.com/corporate/privacy. Throughout this Complaint, Plaintiffs will refer to the 2023 Privacy Policy, as it was in place at the time of the Data Breach. A new Privacy Policy, adopted after the Data Breach, was posted on July 1, 2024, at https://www.caesars.com/corporate/privacy. That new policy directs consumers to a Privacy and Data Protection Policy updated on July 1, 2023, "[t]o review our Privacy Principles or to learn more about how Caesars manages privacy compliance," which is available at https://www.caesars.com/content/dam/corporate/pdfs/privacy-data-protection.pdf.

[10] Rohnan Goswami & Contessa Brewer, *Caesars paid millions in ransom to cybercrime group prior to MGM hack*, CNBC (Sept. 14, 2023), https://www.cnbc.com/2023/09/14/caesars-paid-millions-in-ransom-to-cybercrime-group-prior-to-mgm-hack.html.

[11] *Id.*

was erased.[12]

7. Individuals, including Plaintiffs and Class Members, were customers of Defendant's gaming and entertainment services and/or members of Defendant's Rewards program. By obtaining, using, and deriving a benefit from Plaintiffs' and Class Member' PII, Caesars assumed legal and equitable duties to Plaintiffs and Class Members to safeguard that information and knew, or should have known, that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure. Plaintiffs and Class Members had a reasonable expectation and understanding that Defendant would adopt reasonable data security safeguards to protect PII. Defendant failed to do so, leading to the Data Breach.

8. Caesars owed a non-delegable duty to Plaintiffs and Class Members to implement reasonable and adequate security measures to protect their PII that it chose to collect and keep. Yet, despite knowing of the serious risk of cyberattack it faced, Caesars maintained this PII in a negligent and/or reckless manner and maintained the PII in a condition which left it vulnerable to those cyberattacks.

9. The Data Breach was a direct result of Caesars' failure to implement reasonable

[12] Amaris Encinas, *Caesars Entertainment ransomware attack targeting loyalty members revealed in SEC filing*, USA Today (Sept. 14, 2023), https://www.usatoday.com/story/tech/news/2023/09/14/caesars-entertainment-cyberattack-loyalty-members-data-breach/70856343007/; Caesars' Sample Data Breach Notice, https://attorneygeneral.delaware.gov/wp-content/uploads/sites/50/2023/10/Caesars-AG-Notice-Sample-Notice.pdf. (last visited July 26, 2024). *See also* Lawrence Adams, *Scam PSA: Ransomware gangs don't always delete stolen data when paid*, BleepingComputer (Nov. 4, 2020), https://www.bleepingcomputer.com/news/security/scam-psa-ransomware-gangs-dont-always-delete-stolen-data-when-paid/ ("Companies should automatically assume that their data has been shared among multiple threat actors and that it will be used or leaked in some manner in the future, regardless of whether they paid."); Mathew J. Schwartz, *Ransom Realpolitik: Paying for Data Deletion Is for Suckers*, Bank Info Security (Dec. 1, 2022), https://www.bankinfosecurity.com/ransom-realpolitik-paying-for-data-deletion-for-suckers-a-20596 ("[U]rges victims to never pay for any promise or guarantees to delete data, including for victims in the healthcare sector that might be trying to minimize any impact on patients"); Bill Toulas, *Ransom payments fall as fewer victims choose to pay hackers*, BleepingComputer (July 28, 2022), https://www.bleepingcomputer.com/news/security/ransom-payments-fall-as-fewer-victims-choose-to-pay-hackers/ ("Coveware underlines that in many cases, despite receiving the ransom payment, the threat actors continued the extortion or leaked the stolen files anyway.").

data security measures to protect Class Members' PII against unauthorized intrusions and access.

10. As a result of the Data Breach, Plaintiffs and Class Members have been damaged in several ways. Plaintiffs and Class Members have endured actual and attempted fraud and/or have been exposed to an increased risk of fraud, identity theft, and other misuse of their PII. Plaintiffs and Class Members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. To protect themselves from this increased risk of fraud, Plaintiffs and Class Members may be forced to purchase credit monitoring and other identity protection services, purchase credit reports, place credit freezes and fraud alerts on their credit reports and spend time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class Members have also suffered "benefit of the bargain" damages because they paid money to Caesars for services that were intended to be accompanied by adequate data security but were not. Plaintiffs and Class Members also suffered a "loss of value of PII" resulting from the Data Breach.

11. PII stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources (such as publicly available information, social media, etc.) to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen PII to send spear-phishing emails and text messages to Class Members to trick them into revealing sensitive information such as Social Security numbers, financial account numbers, login credentials, and the like. Thieves can also send emails and text messages embedded with ransomware.

12. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated consumers whose PII was stolen in the Data Breach. Plaintiffs seek remedies including: (i) compensation for the theft and misuse of their data; (ii) reimbursement of out-of-pocket costs; (iii) compensation for time spent responding to the Data Breach; (iv) comprehensive identify protection services paid for by Caesars; and (v) injunctive relief requiring substantial improvements to Caesars' data security practices, including the deletion of Class Members' information from unsecured locations, as detailed below.

II. PARTIES

A. Plaintiffs

1. California Plaintiffs

13. Plaintiff **Dhaman Gill** ("Plaintiff Gill") is a citizen and resident of the state of California. Plaintiff Gill has been a Caesars Reward member during the relevant time period. Plaintiff Gill regularly gambled with Caesars in person and stayed at Caesars resorts, at which time Caesars regularly collected his PII.

14. To obtain his membership, Plaintiff Gill was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Gill was required to provide to obtain his Caesars Rewards membership.

15. On October 11, 2023, Plaintiff Gill learned of the Data Breach from an email communication received from Caesars. Shortly thereafter in October 2023, Plaintiff Gill learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained in Caesars' database.

16. Plaintiff Gill has been careful to protect and monitor his identity. After the Data Breach, Plaintiff Gill purchased his own credit monitoring service (Experian Identity Works) for an annual fee of $400.

17. As a result of the Data Breach, Plaintiff Gill made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: contacting his credit card companies to change cards, contacting his phone company to activate a "spam blocker," purchasing credit monitoring services for $400 per year, monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received 3-5 times every day since the Data Breach. Plaintiff Gill has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has

been lost forever and cannot be recaptured.

18. Despite these efforts, Plaintiff Gill suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (ex. credit monitoring service); (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (x) daily fear and anxiety about what he may face next; (xi) nominal and statutory damages; and (xii) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

19. In addition, as a result of the Data Breach, Plaintiff Gill has experienced multiple attempts of identity theft and fraudulent activity regarding his credit card accounts, including several dozen attempts to withdraw money out of his bank account, an attempt by an unauthorized actor to open an Apple credit card in his name in early 2024, and multiple unauthorized charges made on his credit and debit cards. As a result of this fraudulent conduct, Plaintiff Gill had to change multiple credit cards and multiple banks that he has used since the Data Breach.

20. Plaintiff Gill also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which occur daily, as well receiving notifications from Experian identity works on May 14, 2024, Feb 15, 2024, Jan 11, 2024, Jan 4, 2024, Dec 26, 2023, Dec 18, 2023, and Nov 22, 2023, that his PII was located on the dark web, which, upon information and belief, were caused by the Data Breach.

21. Had Plaintiff Gill been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Gill relied on Caesars' policies and promises to implement

sufficient measures to protect his PII and privacy rights.

22. As a result of the Data Breach, Plaintiff Gill anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

23. Plaintiff Gill has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

24. Plaintiff **Carey Hylton** ("Plaintiff Hylton") is a citizen and resident of the state of California. Plaintiff Hylton has been a Caesars Reward member for at least 10 years. Plaintiff Hylton also currently holds a Caesars credit card, which she obtained in the summer of 2022. Plaintiff Hylton regularly gambled with Caesars both online and in person and has stayed at Caesars hotels at least twice a year for several years, at which time Caesars regularly collected her PII.

25. To obtain her membership, Plaintiff Hylton was required to entrust Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Hylton was required to provide to obtain her Caesars Rewards membership.

26. On or around October 2023, Plaintiff Hylton learned of the Data Breach from a letter sent to her by Caesars, notifying her that Caesars had allowed dangerous criminals to access her PII including her name, driver's license number, social security number, and other data contained in Caesars' database.

27. Plaintiff Hylton has been careful to protect and monitor her identity. Plaintiff Hylton had credit monitoring coverage before the Data Breach with LifeLock, which she obtained in 2021. In response to the Data Breach and threat to her PII, Plaintiff Hylton continued to pay for this service ($10/month for two more months), in addition to an attempt to purchase the credit monitoring service offered by Caesars (but was denied enrollment in such service).

28. As a result of the Data Breach, Plaintiff Hylton made reasonable efforts to mitigate

the impact of the Data Breach, including but not limited to: monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the increase in disruptive scam phone calls, texts, and emails she has received since the Data Breach. Plaintiff Hylton has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

29. Despite these efforts, Plaintiff Hylton suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (late fees she was required to pay for fraudulent Caesars' credit card charges); (ii) damage and loss of the value of her PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of her PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

30. In addition, as a result of the Data Breach, Plaintiff Hylton has experienced several fraudulent credit card charges on her Caesars' credit card, which resulted in her incurring late fees imposed on her by Caesars.

31. Plaintiff Hylton also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

32. Had Plaintiff Hylton been informed that Caesars had insufficient data security measures to protect her PII, she would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Hylton relied on Caesars' policies and promises to

implement sufficient measures to protect her PII and privacy rights.

33. As a result of the Data Breach, Plaintiff Hylton anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

34. Plaintiff Hylton has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

35. Plaintiff **Miguel Rodriguez** ("Plaintiff Rodriguez") is a citizen and resident of the state of California. Plaintiff Rodriguez regularly gambled with Caesars both online and in person, at which time Caesars regularly collected his PII.

36. To obtain his membership, Plaintiff Rodriguez was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Rodriguez was required to provide to obtain his Caesars Rewards membership.

37. On or around September 2023, Plaintiff Rodriguez learned of the Data Breach from media coverage and has not, to date, received a notice letter from Caesars, notifying him of the specific PII of his that was accessed by dangerous criminals through the Data Breach.

38. As a result of the Data Breach, Plaintiff Rodriguez made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to dealing with the numerous specific instances of identity theft and fraudulent activity that he experienced (as detailed below), monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

39. Despite these efforts, Plaintiff Rodriguez suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of his PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of his PII; (v) lost value of

PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) fear of what could happen to his credit; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

40. In addition, as a result of the Data Breach, Plaintiff Rodriguez has suffered actual injury in the form of experiencing numerous fraudulent attempts to open credit or bank accounts on his name, including US Bank notifying him that in October 2023 that someone had attempted to open a US Bank account in his name in Minnesota, which he did not authorize, resulting in Plaintiff Rodriguez needing to close his bank account. Plaintiff Rodriguez has also experienced several unauthorized inquiries that appeared on his credit report.

41. Plaintiff Rodriguez also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving a notification on April 16, 2024, that his PII was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

42. Had Plaintiff Rodriguez been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Rodriguez relied on Caesars' policies and promises to implement sufficient measures to protect her PII and privacy rights.

43. As a result of the Data Breach, Plaintiff Rodriguez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

44. Plaintiff Rodriguez has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded

from future breaches.

2. Illinois Plaintiffs

45. Plaintiff **April Elvidge** ("Plaintiff Elvidge") is a citizen and resident of the state of Illinois. Plaintiff Elvidge has been a Caesars Reward member since January 2021. Plaintiff Elvidge regularly gambled with Caesars both online and in person at which time Caesars regularly collected her PII.

46. To obtain her membership, Plaintiff Elvidge was required to entrust Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Elvidge was required to provide to obtain her Caesars Rewards membership.

47. On or around October 2023, Plaintiff Elvidge learned of the Data Breach from a letter sent to her by Caesars, notifying her that Caesars had allowed dangerous criminals to access her PII including her name, driver's license number, social security number, and other data contained in Caesars' database.

48. Plaintiff Elvidge has been careful to protect and monitor her identity. She had credit monitoring coverage through Capital One at the time that the Caesars' breach was announced.

49. As a result of the Data Breach, Plaintiff Elvidge made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the 10+ disruptive spam phone calls and 3+ spam texts that she receives on a daily basis. Plaintiff Elvidge has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

50. Despite these efforts, Plaintiff Elvidge suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs; (ii) damage and loss of the value of her PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of

her PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

51. Plaintiff Elvidge also suffered actual injury in the form of a significant increase in spam calls (about 10 per day) and spam texts (about 3 per day) and receiving a notification from a credit protection account she uses that her information was located on the dark web.

52. Had Plaintiff Elvidge been informed that Caesars had insufficient data security measures to protect her PII, she would not have enrolled with Caesars Rewards or have gamed or stayed at Caesars as frequently or at all. Plaintiff Elvidge relied on Caesars' policies and promises to implement sufficient measures to protect her PII and privacy rights.

53. As a result of the Data Breach, Plaintiff Elvidge anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

54. Plaintiff Elvidge has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

55. Plaintiff **Charles Popp** ("Plaintiff Popp") is a citizen and resident of the state of Illinois. Plaintiff Popp has been a Caesars Reward member during the relevant time period. Plaintiff Smith regularly gambled with Caesars using its sportsbook app, at which time Caesars regularly collected his PII.

56. To obtain his membership, Plaintiff Popp was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social

Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Popp was required to provide to obtain his Caesars Rewards membership.

57. On or around October 2023, Plaintiff Popp learned of the Data Breach from a letter sent to her by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including her name, driver's license number, social security number, and other data contained in Caesars' database.

58. Plaintiff Popp has been careful to protect and monitor his identity. He had credit monitoring coverage at the time that the Data Breach was announced.

59. As a result of the Data Breach, Plaintiff Popp made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: changing email passwords several times, monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the increase in disruptive scam phone calls, texts, and emails he has received since the Data Breach. Plaintiff Popp has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

60. Despite these efforts, Plaintiff Popp suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs; (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) consistent feelings of anxiety; (v) invasion of privacy; (vi) theft of his PII; (vii) lost value of PII; (viii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) loss of benefit of the bargain; (x) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (xi) nominal and statutory damages; and (xii) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

61. In addition, Plaintiff Popp suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving a notification from Credit Karma approximately six months ago that his PII was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

62. Had Plaintiff Popp been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Popp relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

63. As a result of the Data Breach, Plaintiff Popp anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

64. Plaintiff Popp has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

65. Plaintiff **John Gedwill** ("Plaintiff Gedwill") is a citizen and resident of the state of Illinois. Plaintiff Gedwill has been a Caesars Reward member for at least two years. Plaintiff Gedwill regularly gambled with Caesars both online and in person at which time Caesars regularly collected his PII.

66. To obtain his membership, Plaintiff Gedwill was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Gedwill was required to provide to obtain his Caesars Rewards membership.

67. On or around October 2023, Plaintiff Gedwill learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained in Caesars' database.

68. Plaintiff Gedwill has been careful to protect and monitor his identity. He monitors his credit through Annual Credit Report.com.

69. As a result of the Data Breach, Plaintiff Gedwill made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to telephone conversations with his bank about the Data Breach and protecting his accounts from fraudulent use, monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the disruptive scam phone calls, texts, and emails she has received since the Data Breach.

70. Despite these efforts, Plaintiff Gedwill suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs; (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (x) concern about third parties having access to personal information; (xi) nominal and statutory damages; and (xii) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

71. In addition, as a result of the Data Breach, Plaintiff Gedwill has experienced a phishing attempt in which a stranger sent him money and requested that he return it.

72. Plaintiff Gedwill also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

73. Had Plaintiff Gedwill been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at

Caesars as frequently or at all. Plaintiff Gedwill relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

74. As a result of the Data Breach, Plaintiff Gedwill anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

75. Plaintiff Gedwill has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

76. Plaintiff **Laura McNichols** ("Plaintiff L. McNichols") is a citizen and resident of the state of Illinois. Plaintiff L. McNichols has been a Caesars Reward member during the relevant time period. Plaintiff L. McNichols regularly gambled with Caesars both online and in person at which time Caesars regularly collected her PII.

77. On or around October 2023, Plaintiff L. McNichols learned of the Data Breach from a news article and has not, to date, received a notice letter from Caesars, notifying her of the specific PII of hers that was accessed by dangerous criminals through the Data Breach.

78. To obtain her membership, Plaintiff L. McNichols was required to entrust Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff L. McNichols was required to provide to obtain her Caesars Rewards membership.

79. Plaintiff L. McNichols has been careful to protect and monitor her identity, including through the use of credit monitoring coverage through T-Mobile before the Data Breach.

80. As a result of the Data Breach, Plaintiff L. McNichols made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the disruptive scam phone calls, texts, and emails she has received since the Data Breach.

81. Despite these efforts, Plaintiff L. McNichols suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of her PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of her PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) statutory damages; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

82. In addition, as a result of the Data Breach, Plaintiff L. McNichols has suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving a notification from T-Mobile that her Social Security numbers was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

83. Had Plaintiff L. McNichols been informed that Caesars had insufficient data security measures to protect her PII, she would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff L. McNichols relied on Caesars' policies and promises to implement sufficient measures to protect her PII and privacy rights.

84. As a result of the Data Breach, Plaintiff L. McNichols anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

85. Plaintiff L. McNichols has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

86. Plaintiff **Thomas McNichols** ("Plaintiff T. McNichols") is a citizen and resident of the state of Illinois. Plaintiff T. McNichols has been a Caesars Reward member during the relevant

time period. Plaintiff T. McNichols regularly gambled with Caesars both online and in person at which time Caesars regularly collected his PII.

87. On or around October 2023, Plaintiff T. McNichols learned of the Data Breach from a news article and has not, to date, received a notice letter from Caesars, notifying him of the specific PII of his that was accessed by dangerous criminals through the Data Breach.

88. To obtain his membership, Plaintiff T. McNichols was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff T. McNichols was required to provide to obtain his Caesars Rewards membership.

89. Plaintiff T. McNichols has been careful to protect and monitor his identity, including through the use of credit monitoring coverage through T-Mobile before the Data Breach.

90. As a result of the Data Breach, Plaintiff T. McNichols made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

91. Despite these efforts, Plaintiff T. McNichols suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of his PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of his PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) statutory damages; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

92. In addition, as a result of the Data Breach, Plaintiff T. McNichols has suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving a notification from T-Mobile that his Social Security numbers was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

93. Had Plaintiff T. McNichols been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed or stayed at Caesars as frequently or at all. Plaintiff T. McNichols relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

94. As a result of the Data Breach, Plaintiff T. McNichols anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

95. Plaintiff T. McNichols has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

96. Plaintiff **Virginia Stacy** ("Plaintiff Stacy") is a citizen and resident of the state of Illinois. Plaintiff Stacy has been a Caesars Reward member during the relevant time period. Plaintiff Stacy regularly gambled with Caesars both online and in person, at which time Caesars regularly collected her PII.

97. On or around October 2023, Plaintiff Stacy learned of the Data Breach from a letter sent to her by Caesars, notifying her that Caesars had allowed dangerous criminals to access her PII including his name, driver's license number, social security number, and other data contained in Caesars' database.

98. To obtain her membership, Plaintiff Stacy was required to entrust Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Stacy was required to provide to obtain her Caesars Rewards membership.

99. Plaintiff Stacy has been careful to protect and monitor her identity, including

through the use of credit monitoring coverage Credit Wise and Capital One.

100. As a result of the Data Breach, Plaintiff Stacy made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to taking actions to prevent numerous attempts of fraudulent activity that she experienced (as detailed below), freezing her credit, monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the disruptive scam phone calls, texts, and emails she has received since the Data Breach.

101. Despite these efforts, Plaintiff Stacy suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of her PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of her PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) statutory damages; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

102. In addition, as a result of the Data Breach, Plaintiff Stacy has suffered actual injury in the form of an unauthorized actor opening a credit card in her name that was used to attempt to purchase a car and a Verizon phone.

103. Had Plaintiff Stacy been informed that Caesars had insufficient data security measures to protect her PII, she would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Stacy relied on Caesars' policies and promises to implement sufficient measures to protect her PII and privacy rights.

104. As a result of the Data Breach, Plaintiff Stacy anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data

Breach.

105. Plaintiff Stacy has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

106. Plaintiff **Edward Cherveny** ("Plaintiff Cherveny") is a citizen and resident of the state of Illinois. Plaintiff Cherveny has been a Caesars Reward member during the relevant time period. Plaintiff Cherveny regularly gambled with Caesars in person at which time Caesars regularly collected his PII.

107. To obtain his membership, Plaintiff Cherveny was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Cherveny was required to provide to obtain his Caesars Rewards membership.

108. On or around October 2023, Plaintiff Cherveny learned of the Data Breach from an email communication sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained in Caesars' database.

109. As a result of the Data Breach, Plaintiff Cherveny made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

110. Despite these efforts, Plaintiff Cherveny suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of his PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of his PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) statutory

damages; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

111. Plaintiff Cherveny also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails since the Data Breach, which, upon information and belief, was caused by the Data Breach.

112. Had Plaintiff Cherveny been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Cherveny relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

113. As a result of the Data Breach, Plaintiff Cherveny anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

114. Plaintiff Cherveny has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

3. Indiana Plaintiffs

115. Plaintiff **James Martin** ("Plaintiff Martin") is a citizen and resident of the state of Indiana. Plaintiff Martin has been a Caesars Reward member during the relevant time period. Plaintiff Martin regularly gambled with Caesars in person and stayed at Caesars resorts, at which time Caesars regularly collected his PII.

116. To obtain his membership, Plaintiff Martin was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Martin was required to provide to obtain his Caesars Rewards

membership.

117. On or around October 2023, Plaintiff Martin learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained in Caesars' database.

118. Plaintiff Martin has been careful to protect and monitor his identity. In fact, Plaintiff Martin discovered the Data Breach on his own, before information was released to him from Caesars. Before receiving any notice of the data breach, Mr. Martin sent Caesars a letter (dated September 18, 2023), informing them about suspicious activity and a suspected data breach, including massive increase in spam emails he was receiving, and attempts to put him on the dark web. He never once received a response from Caesars. After collecting this evidence of suspicious activity and sending it to Caesars, Plaintiff Martin saw the Data Breach on the news. Shortly after the Data Breach, Plaintiff Martin purchased the Equifax credit monitoring service for $89/year.

119. As a result of the Data Breach, Plaintiff Martin made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to closing accounts and opening new accounts (and get all new credit cards), making several attempts to communicate with Caesars about the Data Breach before it was publicly announced, addressing multiple alerts received by Experian about attempted attacks made to his credit report and having Experian lock his credit report as a result of such attempts, monitoring his credit card and checking account statements for any signs of fraudulent activity, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

120. Despite these efforts, Plaintiff Martin suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) several hundred dollars in out-of-pocket costs; (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences

of the Data Breach; (x) significant levels of stress (as someone living with advanced cancer and other health conditions, this affects his stress and blood pressure and in turn exacerbates his health conditions to an extreme extent); (xi) nominal and statutory damages; and (xii) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

121. In addition, as a result of the Data Breach, Plaintiff Martin has experienced multiple attempts by unauthorized actors to use his bank account and credit cards, requiring him to close multiple bank and credit card accounts. Plaintiff Martin has also experienced a multitude of attempts by bad actors to obtain addition PII from him, as he has been bombarded with spam and phishing calls, texts, and emails by bad actors pretending to be affiliated with Caesars and requesting he provide PII and financial information. As a result of this fraudulent activity that took place after the Data Breach, Plaintiff Martin was compelled to change his phone number, which cost him $150, and pay for Equifax credit monitoring, which costs him $89/year.

122. Plaintiff Martin also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and notifications that his PII was discovered on the dark web, which, upon information and belief, were caused by the Data Breach.

123. Had Plaintiff Martin been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Martin relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

124. Plaintiff Martin has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

4. Minnesota Plaintiffs

125. Plaintiff **Cynthia Rubner** ("Plaintiff C. Rubner") is a citizen and resident of the

state of Minnesota. Plaintiff C. Rubner has been a Caesars Reward member during the relevant time period. Plaintiff C. Rubner regularly stayed at Caesars' resorts, at which time Caesars regularly collected her PII.

126. To obtain her membership, Plaintiff C. Rubner was required to entrust Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff C. Rubner was required to provide to obtain her Caesars Rewards membership.

127. On or around October 2023, Plaintiff C. Rubner learned of the Data Breach from a letter sent to her by Caesars, notifying her that Caesars had allowed dangerous criminals to access her PII including her name, driver's license number, social security number, and other data contained in Caesars' database.

128. As a result of the Data Breach, Plaintiff C. Rubner made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to contacting Caesars' customer service in an attempt to learn more about the Data Brach, calling her bank to inform them of the breach, and checking bank statements for herself and her husband about three times daily.

129. Despite these efforts, Plaintiff C. Rubner suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of her PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of her PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) anxiety and constant worry of being victim to identity theft; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

130. In addition, Plaintiff C. Rubner has also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

131. Had Plaintiff C. Rubner been informed that Caesars had insufficient data security measures to protect her PII, she would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff C. Rubner relied on Caesars' policies and promises to implement sufficient measures to protect her PII and privacy rights.

132. As a result of the Data Breach, Plaintiff C. Rubner anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

133. Plaintiff C. Rubner has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

134. Plaintiff **William Rubner** ("Plaintiff W. Rubner") is a citizen and resident of the state of Minnesota. Plaintiff W. Rubner has been a Caesars Reward member for at least four years. Plaintiff W. Rubner regularly stayed at Caesars resorts, at which time Caesars regularly collected his PII.

135. To obtain his membership, Plaintiff W. Rubner was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff William Rubner was required to provide to obtain his Caesars Rewards membership.

136. On or around October 2023, Plaintiff W. Rubner learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access her PII including his name, driver's license number, social security number, and other data contained in Caesars' database.

137. Plaintiff W. Rubner has been careful to protect and monitor his identity, including

through the use of credit monitoring coverage LifeLock.

138. As a result of the Data Breach, Plaintiff W. Rubner made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

139. Despite these efforts, Plaintiff W. Rubner suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of his PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of his PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) statutory damages; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

140. Plaintiff W. Rubner also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving a notification from LifeLock since the Data Breach that his PII was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

141. Had Plaintiff W. Rubner been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff W. Rubner relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

142. As a result of the Data Breach, Plaintiff W. Rubner anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

143. Plaintiff W. Rubner has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

5. New York Plaintiffs

144. Plaintiff **Crystal Brewster** ("Plaintiff Brewster") is a citizen and resident of the state of New York. Plaintiff Brewster has been a Caesars Reward member for at least ten years. Plaintiff Brewster regularly gambled with Caesars both online and in person, at which time Caesars regularly collected her PII.

145. To obtain her membership, Plaintiff Brewster was required to entrust Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Brewster was required to provide to obtain his Caesars Rewards membership.

146. On or around October 2023, Plaintiff Brewster learned of the Data Breach from a letter sent to her by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including her name, driver's license number, social security number, and other data contained in Caesars' database.

147. Plaintiff Brewster has been careful to protect and monitor her identity. She paid $24.99/month for credit monitoring coverage at the time of the Data Breach.

148. As a result of the Data Breach, Plaintiff Brewster made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: changing her telephone number, monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the disruptive scam phone calls, texts, and emails she has received 3-5 times every day since the Data Breach. Plaintiff Brewster has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

149. As a result of the Data Breach, Plaintiff Brewster made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to attempting to contact Caesars at the beginning of the breach. She has also spent time reviewing account statements closely, logging into online accounts to check activity, signing up for credit monitoring, obtaining credit freezes, obtaining credit reports, researching news coverage about the breach, reading breach news almost daily. She visited her bank (over 1,000 miles over 9 months) and reset her billing.

150. Despite these efforts, Plaintiff Brewster suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs; (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of her PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (x) heightened anxiety; (xi) nominal and statutory damages; and (xii) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

151. In addition, since the Data Breach, Plaintiff Brewster has experienced constant and repeated attempts of identity theft and fraud which did not occur before the Data Breach, including: (i) a Fortiva credit card being opened in her name of which she had no knowledge; (ii) multiple inquiries made in her name to open automobile loans that she knew nothing about; (iii) an authorized charge appearing on her Bank of America account which she was forced to dispute; (iv) receiving a notice attempting to illicit payment from her based on claims that she was past due on payments owed to Verizon Wireless, despite her not having a Verizon account; (v) being compelled to close multiple bank accounts with Bank of America and Merryl Lynch due to frequent unauthorized charges being made; (vi) being compelled to change her telephone number due to the frequency of spam communications she has received since the Data Breach; and (vii)

changing her name due to the above attempted acts of identity theft and fraud that have taken place since the Data Breach.

152. Plaintiff Brewster also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

153. Had Plaintiff Brewster been informed that Caesars had insufficient data security measures to protect his PII, she would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Brewster relied on Caesars' policies and promises to implement sufficient measures to protect her PII and privacy rights.

154. As a result of the Data Breach, Plaintiff Brewster anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

155. Plaintiff Brewster has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

156. Plaintiff **Isaac Dwek** ("Plaintiff Dwek") is a citizen and resident of the state of New York. Plaintiff Dwek has been a Caesars Reward member during the relevant time period. Plaintiff Dwek regularly gambled with Caesars both online and in person, at which time Caesars regularly collected his PII.

157. To obtain his membership, Plaintiff Dwek was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Dwek was required to provide to obtain his Caesars Rewards membership.

158. On or around October 2023, Plaintiff Dwek learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained

in Caesars' database.

159. Plaintiff Dwek has been careful to protect and monitor his identity. At the time of the Data Breach, Plaintiff Dwek used a Credit Karma credit monitoring service. Plaintiff Dwek had used this service since about 2014.

160. As a result of the Data Breach, Plaintiff Dwek made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received 3-5 times every day since the Data Breach. Plaintiff Dwek has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

161. Despite these efforts, Plaintiff Dwek suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of his PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of his PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) stress of knowing that his personal information is "out there"; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

162. In addition, Plaintiff Dwek has also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

163. Had Plaintiff Dwek been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at

Caesars as frequently or at all. Plaintiff Dwek relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

164. As a result of the Data Breach, Plaintiff Dwek anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

165. Plaintiff Dwek has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

6. Pennsylvania Plaintiffs

166. Plaintiff **Monica Blair-Smith** ("Plaintiff Smith") is a citizen and resident of the commonwealth of Pennsylvania. Plaintiff Smith has been a Caesars Reward member during the relevant time period. Plaintiff Smith regularly gambled with Caesars and booked hotel rooms with it online and in-person, at which time Caesars regularly collected her PII.

167. To obtain her membership, Plaintiff Smith was required to entrust Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Smith was required to provide to obtain her Caesars Rewards membership.

168. On or around October 2023, Plaintiff Smith learned of the Data Breach on her own and has not, to date, received a notice letter from Caesars, notifying her of the specific PII of hers that was accessed by dangerous criminals through the Data Breach.

169. As a result of the Data Breach, Plaintiff Smith made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the increase in disruptive scam phone calls, texts, and emails she has received since the Data Breach. Plaintiff Smith has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

This time has been lost forever and cannot be recaptured.

170. Despite these efforts, Plaintiff Smith suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of her PII; (ii) anxiety and concern over whether her information has been shared on the dark web; (iii) invasion of privacy; (iv) theft of her PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) nominal and statutory damages; and (x) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

171. Plaintiff Smith also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

172. Had Plaintiff Smith been informed that Caesars had insufficient data security measures to protect her PII, she would not have enrolled with Caesars Rewards or have gamed or stayed at Caesars as frequently or at all. Plaintiff Smith relied on Caesars' policies and promises to implement sufficient measures to protect her PII and privacy rights.

173. As a result of the Data Breach, Plaintiff Smith anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

174. Plaintiff Smith has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

175. Plaintiff **Todd Katz** ("Todd Katz") is a citizen and resident of the commonwealth of Pennsylvania. Plaintiff Katz has been a Caesars Reward member for at least four years. Plaintiff

Katz regularly gambled with Caesars in person at which time Caesars regularly collected his PII.

176. To obtain his membership, Plaintiff Katz was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Katz was required to provide to obtain his Caesars Rewards membership.

177. On or around October 2023, Plaintiff Katz learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained in Caesars' database.

178. As a result of the Data Breach, Plaintiff Katz made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to dealing with the numerous specific instances of identity theft and fraudulent activity that he experienced (as detailed below), monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

179. Despite these efforts, Plaintiff Katz suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of his PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of his PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) statutory damages; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

180. In addition, as a result of the Data Breach, Plaintiff Katz has experienced numerous

fraudulent transactions made on his credit card since the Data Breach, as recently as three months ago, wherein he was alerted by both AMEX and Citizens Bank regarding suspicious charges that were made by an unauthorized person.

181. Had Plaintiff Katz been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Katz relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

182. As a result of the Data Breach, Plaintiff Katz anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

183. Plaintiff Katz has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

7. Texas Plaintiffs

184. Plaintiff **Mark Huddleston** ("Plaintiff Huddleston") is a citizen and resident of the state of Texas. Plaintiff Huddleston has been a Caesars Reward member since 2007. Plaintiff Huddleston regularly gambled with Caesars both online and in person at which time Caesars regularly collected his PII.

185. To obtain his membership, Plaintiff Huddleston was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Huddleston was required to provide to obtain his Caesars Rewards membership.

186. On or around September 11, 2023, Plaintiff Huddleston learned of the Data Breach from news reports, though he was unsure of whether his PII had been compromised. On October 19, 2023, Plaintiff Huddleston learned of the Data Breach from a news article and has not, to date, received a notice letter from Caesars, notifying him of the specific PII of his that was accessed by dangerous criminals through the Data Breach.

187. Plaintiff Huddleston has been careful to protect and monitor his identity. He accepted the free credit monitoring option suggested by Caesars, though he had difficulties registering.

188. As a result of the Data Breach, Plaintiff Huddleston made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to dealing with the numerous specific instances of identity theft and fraudulent activity that he experienced (as detailed below), monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

189. Despite these efforts, Plaintiff Huddleston suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of his PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of his PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) fear of what could happen to his credit; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

190. In addition, as a result of the Data Breach, Plaintiff Huddleston has suffered actual injury in the form of experiencing numerous fraudulent attempts to open credit or bank accounts on his name, including lines of credit, that have impacted his credit score, and numerous unauthorized account inquires. For example, on September 14, 2023, Plaintiff Huddleston received a notification from US Alliance, thanking him for applying for an account that he never applied for, and on September 12, 2023, he received a message from BHG Financial, stating that it reviewed his credit-file and was ready to get him approved for a loan that he never applied for.

191. Plaintiff Huddleston also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving numerous notifications since September 2023, from Capital One, IDX, Experian, and Credit Karma that his PII was compromised and/or discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

192. Plaintiff Huddleston also experienced actual fraud on September 13, 2023, when someone attempted to open an account with Verna Payments using the same type of information that was taken in the Data Breach.

193. Had Plaintiff Huddleston been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all. Plaintiff Huddleston relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

194. As a result of the Data Breach, Plaintiff Huddleston anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

195. Plaintiff Huddleston has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

8. Virginia Plaintiffs

196. Plaintiff **David Lackey** ("Plaintiff Lackey") is a citizen and resident of the state of Virginia. Plaintiff Lackey has been a Caesars Reward member during the relevant time period. Plaintiff Lackey regularly gambled with Caesars as well as having stayed at Caesars resorts, at which time Caesars regularly collected his PII.

197. To obtain his membership, Plaintiff Lackey was required to entrust Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff was required to provide to obtain his Caesars Rewards membership.

198. On or around September 2023, Plaintiff Lackey learned of the Data Breach from a

friend, and then from news reports though he was unsure of whether his PII had been compromised. On October 16, 2023, Caesars sent Plaintiff Lackey formal notice that it had allowed dangerous criminals to access his PII including, "among other data," his name, driver's license or other government issued ID number, and social security number.

199. As a result of the Data Breach, Plaintiff Lackey made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the increase in disruptive scam phone calls, texts, and emails he has received since the Data Breach. Plaintiff Lackey has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

200. Despite these efforts, Plaintiff Lackey suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) damage and loss of the value of his PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of his PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) fear of identity theft; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

201. In addition, Plaintiff Lackey has also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

202. Had Plaintiff Lackey been informed that Caesars had insufficient data security measures to protect his PII, he would not have enrolled with Caesars Rewards or have gamed at

Caesars as frequently or at all. Plaintiff Lackey relied on Caesars' policies and promises to implement sufficient measures to protect his PII and privacy rights.

203. As a result of the Data Breach, Plaintiff Lackey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

204. Plaintiff Lackey has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Caesars' possession, is protected and safeguarded from future breaches.

B. Defendant

205. Defendant Caesars Entertainment, Inc. is a publicly traded company incorporated in Delaware with its principal place of business at 100 West Liberty Street, 12th Floor, Reno, NV 89501. It is a global hospitality and gaming company that owns, operates, and manages hotels, casinos, and resorts located predominantly in Nevada. Caesars' portfolio of Las Vegas properties includes Caesars' Place Las Vegas, The Cromwell, Flamingo Las Vegas, Horseshoe Las Vegas, The LINQ Hotel & Casino, Paris Las Vegas, Planet Hollywood Resort & Casino, Harrah's Las Vegas, and Rio All-Suite and Casino.[13] Caesars' net revenue in 2022 was approximately $10 billion and net income was approximately $1 billion.

III. JURISDICTION AND VENUE

206. This Court has subject matter jurisdiction over the action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs, there are more than 100 Class Members, and several Plaintiffs and at least one Class member is a citizen of a state different than Defendant.

207. This Court has general personal jurisdiction over Caesars because Caesars maintains its principal place of business in this District. This Court also has specific personal

[13] *See* Caesars Entertainment, Inc. Form 10-K for the year ended Dec. 31, 2022, at 28 (Feb. 21, 2023), *available at* https://investor.caesars.com/static-files/abff6ce9-34b1-4057-9c78-db6bf146c295.

jurisdiction over Caesars because Caesars engaged in the conduct underlying this action in this District, including the collection, storage, and inadequate safeguarding of Plaintiffs' PII.

208. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Caesars is based in this District, entered into consumer transactions with Plaintiffs in this District, and made its data security decisions leading to the Data Breach in this District.

IV. STATEMENT OF FACTS

A. Caesars' Business

209. Caesars, formally known as Eldorado Resorts, operates more than 50 casino gaming and resort properties throughout the United States.

210. Caesars' loyalty program, Caesars Rewards, allows members to earn credits by betting on casino games, races, and sports games, both online and at Caesars' various properties, including on the Las Vegas Strip, and redeem them for more gaming or for hotel reservations, dining, shopping, and/or spa services.[14]

211. Plaintiffs and Class Members are current and former Caesars Rewards members.

212. As a condition of receiving its products and/or services, Caesars requires that its Caesars Rewards members, including Plaintiffs and Class Members, entrust it with highly sensitive personal information such as their full legal name, full address, date of birth, drivers' license number, and Social Security number.

213. The information held by Caesars in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

214. Caesars made promises and representations to its customers, including Plaintiffs and Class Members, that the PII collected from them as a condition of obtaining membership in the Caesars Rewards program would be kept safe, confidential, that the privacy of that information would be maintained, and that Caesars would delete any sensitive information after it was no

[14] Caesars Entertainment, Who We Are, https://www.caesars.com/corporate (last visited July 19, 2024).

longer required to maintain it.

215. Caesars' 2023 Privacy Policy provides that it is "committed to respecting your data privacy," and that it "maintain[s] physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control."[15]

216. Plaintiffs and Class Members provided their PII to Caesars with the reasonable expectation and on the mutual understanding that Caesars would comply with its obligations to keep such information confidential and secure from unauthorized access.

217. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Caesars to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

218. Caesars had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Caesars has a legal duty to keep consumer's PII safe and confidential.

219. Caesars had obligations created by the FTC Act, state law, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

220. Caesars derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Caesars could not perform the services it provides. Plaintiffs' and Class Members' PII has an independent value to Caesars.

221. Because of its use of Plaintiffs' and Class Members' PII, Caesars sold more services

[15] 2023 Privacy Policy, *available at* https://web.archive.org/web/20230825011104/https:/www.caesars.com/corporate/privacy. This part of the 2023 Privacy Policy remains unchanged in the Current Privacy Policy.

and products than it otherwise would have.

222. Caesars was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create using Plaintiffs' and Class Members' PII to the detriment of Plaintiffs and Class Members.

223. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Caesars assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

B. The Caesars Data Breach

224. On August 18, 2023, a hacking group, known as Scattered Spider (or UNC3944), gained access to the Caesars Rewards member database and downloaded the unencrypted PII of a significant number of Caesars Rewards 56 million members on or around August 23, 2023.[16] Scattered Spider is known for using social engineering to trick employees of the target company into granting them access to their network.[17] Scattered Spider threat actors monetize access to victim networks in numerous ways including extortion-enabled ransomware and data theft.[18] Thus, they may double-dip: force the target to pay to decrypt their data, while they also sell the exfiltrated data.

225. Scattered Spider gained access to Caesars' inadequately secured data IT network through a social engineering attack on an outsourced IT support vendor used by the Company. Caesars identified the suspicious activity on August 18, 2023, yet Scattered Spider downloaded the unencrypted PII five days later. Caesars did not disclose the Breach to the public or affected

[16] Office of the Maine Attorney General Data Breach Notification, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml (last visited July 19, 2024); Whittaker, *supra* n. 1.

[17] Whittaker, *supra* n. 1.

[18] Cybersecurity & Infrastructure Security Agency, Cybersecurity Advisory, "Scattered Spider," (AA23-320A) (Nov. 16, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a (last visited July 28, 2024).

individuals for three weeks.

226. As reported, Caesars may have paid about $15 million, about half the ransom demand, to Scattered Spider as ransom following the Data Breach.[19]

227. On September 7, 2023, Caesars internal investigation confirmed that Scattered Spider had acquired, among other data, a copy of its loyalty program database including: names, driver's license numbers, and Social Security numbers for a significant number of Caesars Rewards' tens of millions of members.[20]

228. On or around September 14, 2023, Caesars filed a Form 8-K with the SEC to alert investors and shareholders that the Data Breach represented a material event that could materially affect the value of the company.[21]

229. Around that time, Caesars put up a website regarding the Data Breach. The website lacked critical details about the scope and breadth of the Data Breach, but acknowledged that *at a minimum* the driver's license numbers and Social Security numbers of Caesars Rewards members had been accessed and copied.[22] Caesars stated that it was offering credit monitoring and identity theft protection services to all loyalty program members. Caesars also instructed members that they should regularly monitor their credit reports and account statements to protect themselves against identify theft after the breach. However, Caesars did not adequately inform victims that their private information had been breached and instead placed the burden on loyalty members to

---

[19] Thomas Barrabi, *Caesar's Entertainment paid about $15m to hackers who stole customer Social Security numbers, other info: report*, N.Y. Post (Sept. 14, 2023, 2:24 PM), https://nypost.com/2023/09/14/caesars-entertainment-paid-about-15m-to-hackers-who-stole-customer-social-security-numbers-other-info-report/.

[20] Ken Ritter, *Casino giant Caesars Entertainment hit by cyberattack, joining rival MGM Resorts as victim of data breach*, Fortune (Sept. 14, 4:02 AM), https://fortune.com/2023/09/15/caesars-entertainment-cyberattack-mgm-resorts-data-breach/.

[21] *See* Caesars Entertainment, Inc. Form 8-K, Report of unscheduled material events or corporate event (Sept. 14, 2023), *supra* n. 2.

[22] *See* Caesars Entertainment, *Caesars Informational Website*, IDX (now removed), web.archive.org/web/20230914191948/https://response.idx.us/caesars/.

investigate what happened and possibly stumble onto its informational website.

230. Stunningly, Caesars waited until sometime between October 6 and 18, 2023 to officially notify states' attorneys general's offices[23] and send individual notice to the affected Caesars Rewards members that their PII was included in the Breach.[24] This delay exacerbated the harm to Class Members by preventing them from taking steps to mitigate Caesars failures and trying to protect themselves.

231. In the notice to members, Caesars once again counseled them "to be vigilant [against identity theft and fraud] by regularly reviewing your account statements and monitoring any available credit reports for suspicious activity. We also generally encourage you to take care in identifying calls, emails or SMS texts that appear to be spam or fraudulent (e.g., phishing), and to avoid opening links or attachments sent from untrusted sources."[25]

232. The 8-K, website statement, and standard notice leave crucial questions unanswered. Caesars has not, to this date, disclosed: how many of its loyalty rewards program members were affected by the Data Breach; what information was taken; how the cybercriminals were able to exploit vulnerabilities in Caesars' data systems; the identity of Caesars' outside IT vendor; the identity of the hacking group responsible for the Data Breach; or what steps Caesars has taken to ensure that such an attack does not happen again.

233. Although Caesars still has not disclosed precisely the precise nature and scope of the data exfiltrated in the Data Breach, upon information and belief, the data likely consists of PII including names, addresses, phone numbers, email addresses, and dates of birth, as well as driver's

[23] California (report date: 10/11/2023, unreported number of residents effected); Delaware (10/06/2023, 154,611 residents); Hawaii (10/11/2023, 165,271 residents); Indiana (10/06/2023, 1,662,718 residents); Iowa (10/06/2023, 384,087 residents); Massachusetts (10/11/2023, 327,948 residents); Montana (10/06/2023, unreported); Maine (10/06/2023, 41,397 residents); Oregon (10/18/2023, unreported); Texas (unknown report date, 3,381,410 residents); Washington (10/06/2023, 784,234 residents).

[24] Caesars' Sample Data Breach Notice, *supra* n. 12.

[25] *Id.*

license numbers, and Social Security numbers.[26] Cybersecurity journalists have characterized PII stolen in a 2019 breach of Caesars competitor MGM as providing a "treasure trove" of "highly sensitive" personal information, and that affected consumers now face a risk of misuse of their PII.[27] Yet, at this time, Caesars has still not disclosed the number of individuals impacted by the Data Breach, or precisely what forms of PII were taken.

234. As a multi-billion-dollar publicly traded company, Caesars had the financial wherewithal and personnel necessary to prevent the Data Breach. Yet, Caesars nevertheless failed to adopt adequate data security measures.

C. Caesars Uses Consumers' PII for Profit-Generating Purposes

235. Consumers' PII is also valuable to Caesars. Caesars recognizes the business value of PII and collects it to better target customers and increase its profits.

236. Indeed, as a condition of joining Caesars' loyalty program, Caesars requires that its customers entrust it with highly sensitive PII. Caesars retains and stores this information to use for marketing purposes, to develop new products and services, to do statistical analysis, and many other things.[28]

237. Caesars acknowledges in its privacy policy that it uses consumers' PII for the following purposes:

- to operate our Caesars Rewards program and provide information to you about your Caesars Rewards program activity;

[26] Zeba Siddiqui, *Hackers say they stole 6 terabytes of data from casino giants MGM, Caesars*, Reuters (Sept. 14, 2023, 3:16 PM), https://www.reuters.com/business/casino-giant-Caesars-confirms-data-breach-2023-09-14/.

[27] *See* Catalin Cimpanu, *Exclusive: Details of 10.6 million MGM hotel guests posted on a hacking forum*, ZDNet (Feb. 19, 2020, 3:27 PM), https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/; *accord* Chris Morris, *MGM Resorts hack exposes details of 10.6 million guests*, Fortune (Feb. 20, 2020, 9:58 AM), https://fortune.com/2020/02/20/mgm-resorts-hack-data-breach-10-6-million-guests/ ("Identity theft is the big threat here.").

[28] Caesars Entertainment, U.S. Privacy Policy, https://www.caesars.com/corporate/privacy (last visited July 26, 2024).

- to improve the products and services we provide you and develop new products and services;
- to improve our properties, websites and mobile apps;
- to track your use of our properties, websites and mobile apps for our internal market research and analytics;
- to create a more accurate and complete customer profile for you to better understand and predict the products and services you want to use and to provide a more personalized level of service;
- to notify you about promotions and special offers regarding products and services provided by us or our affiliates or other associated third parties, including our business partners;
- to ask for your participation in our internal market research;
- to generate aggregate statistical studies about our customers to better understand how our customers use our services;
- to contact you in response to your inquiries, comments and suggestions;
- to provide a healthy, secure, and safe environment for our customers or employees;
- to protect and defend our rights or property or enforce our agreements with you;
- to perform background checks for any reason (to the extent permitted by applicable laws), which includes but is not limited to any investigation into your identity, any credit checks or any inquiries into your personal history:
- to cash your checks, extend you credit, process credit card, ACH and/or other financial transactions;
- administer general recordkeeping for financial statements and audits;
- comply with our internal records management policy and retention rules;
- to contact you otherwise when necessary; and
- otherwise with your consent or as permitted or required by law.[29]

238. Caesars' self-serving motive to retain and mine its customers' PII for its own financial benefit led to Caesars holding a trove of customer data. Caesars was unjustly enriched by retaining consumers' PII for its own profit motive, while failing to adopt reasonable data security measures to protect that PII.

D. Caesars' Privacy Policy Represents That It Will Adequately Protect PII

239. Caesars' Privacy Policy on its website at the time of the Data Breach touted its data

[29] *See* 2023 Privacy Policy, *supra* n. 15.

security safeguards. The Privacy Policy made materially false and misleading representations and omissions to Class Members. This version of Caesars' Privacy Policy stated the following, in relevant part:

Caesars Entertainment, Inc.
U.S. Privacy Policy

> Caesars Entertainment, Inc. and its subsidiaries and affiliates . . . value you as a customer and are committed to respecting your data privacy. In the course of providing you with products and services, we may collect certain information from or about you. We are providing this Privacy Policy to explain our practices and policies for collecting, using and sharing information collected from or about you when you visit, access, or use, or provide information to us in connection with, one of our properties, websites or mobile Apps (referred to together as the "Caesars Services"). By visiting, accessing, or using, or providing information to us in connection with, the Caesars Services, you expressly consent to our collection, storage, use and sharing of your information as described in this Privacy Policy.
>
> * * *
>
> **INFORMATION WE MAY COLLECT.**
>
> We collect and use information we believe is necessary to administer and promote our business, provide you with the products and services you request, and to provide a safe and healthy environment to our employees and other customers. We may collect and maintain both personal information and non-personal information needed for these purposes. Your personal information and/or non-personal information will be referred as your "information" in this Privacy Policy.
>
> * * *
>
> **HOW WE COLLECT YOUR INFORMATION.**
>
> *Information You Directly Provide to Us*. You may provide information directly to us under a wide range of circumstances, such as when you submit information to us through our websites or mobile apps, use any gaming or non-gaming services at one of our properties, sign up to receive email or text messages from us, sign up to access Wi-Fi at a property, park at a property, install or use one of our mobile apps, sign up for Caesars Rewards, log in as a Caesars Rewards member, book a reservation for a property, enter an online promotion, request information from us, scan your ID at check-in kiosk at a property, apply for casino credit or provide feedback in a survey.

Information Automatically Collected Through the Caesars Websites.

(i) Traffic Data. We automatically track and collect general log information when you visit a website, including your: (A) Internet Protocol (IP) address, (B) domain server, (C) operating system, and (D) type of Web browser as well as the pages you visit on the website (collectively "**Traffic Data**"). Traffic Data does not personally identify you, however, if you choose to provide us with personal information, we may store some items of your personal information and use it with the Traffic Data to better personalize your experience on our websites. We use the Traffic Data to report aggregated website activity and to better understand the needs of our users so we can make informed decisions regarding the content and design of our websites. It enables us to do the following:

- estimate our audience size and usage pattern;
- learn what information is of most and least interest;
- speed up your searches; and
- learn of any possible website performance problems.

We, or our service providers, may also use Traffic Data to identify your physical location to confirm that you are in a jurisdiction where you can use our mobile or online gaming services. We may collect Traffic Data through various technologies including, but not limited to, cookies, IP addresses, and transparent GIFs (Graphics Interchange Format, a software technology also known as a pixel tag).

(ii) Data Collected Using Cookies and Other Technologies. We also automatically collect information from you using cookies and other technologies on our websites. Cookies are small text files offered to your computer by servers in order to keep track of your browser as you navigate a website. Cookies may be stored on your hard drive in which case they remain on your hard drive until deleted, or in temporary memory in which case they are deleted when you shut down your browser or turn off your computer. We may use cookies and similar technologies to identify who you are and may use them when you visit a website, click on our ads, or open our emails. Cookies also enable us to remember your user preferences for our websites. Cookies and other technologies may also be used for site maintenance and analysis, performing network communications, authenticating users, serving contextual advertisements, and protecting against fraud and theft. You can block or remove cookies using your Internet browser's settings. If you block or remove cookies, your ability to perform certain transactions, use certain functionality, and access certain content on the Caesars Websites may be affected. To find out more about cookies, including how to see what cookies have been set on your device and how to manage and delete them, visit www.allaboutcookies.org.

* * *

(vi) Information You Post on the Caesars Websites. If you post information on any public areas of our websites, that information may be collected and used by Caesars, other website users, and the public generally. We strongly recommend that you do not post any information on our websites that allows strangers to identify or locate you or that you otherwise do not want to share with the public.

* * *

Information We Automatically Collect Through Our Mobile Apps, including Location Information. If you install or use one of our mobile apps, we may collect and use information regarding your mobile device, including but not limited to technical information about your mobile device, system and application software, and peripherals, that is gathered periodically to facilitate any upgrades, product support and other services to you (if any) related to the mobile apps, and to provide services or technologies to you. In addition, if you install one of our mobile apps and allow your device to share location information with us, we may be able to automatically identify and collect the location of your mobile device, including GPS location, which is the real-time geographic location of your mobile device. We may use your location information for any of the reasons disclosed in this Privacy Policy, including, for example, to provide you with more relevant content and useful app features, such as wayfinding services at our properties, or to confirm that you are located in a jurisdiction where you can use our mobile gaming services. We may also use this data for statistical or business-related purposes to improve our products, services and properties. If you allow a mobile app to send you push notifications, your location information may be used to send real-time offers for goods and services at our properties that are close to your location. You may adjust your device settings to turn off push notifications at any time. Location information may also be collected and used to tailor your marketing offers to your specific interests. You may choose not to share your location details with us by adjusting or turning off your mobile device's location services settings. Please note that even if you adjust the settings in your mobile device to turn off location sharing (via GPS data), we may be able to collect information about the location of your mobile device if you are located on one of the Caesars properties through your Wi-Fi, Bluetooth, and other device settings. See "Information We Automatically Collect from Mobile Devices on Caesars Properties" below for more information.

Information We Automatically Collect When You Use Our Wi-Fi Services. If you use Wi-Fi services that we make available at one of our properties, we might collect information about your use of our Wi-Fi services, including your IP address, Wi-Fi information (such as SSID), mobile carrier, the websites you visit, the type of device and browser you are using, your device identification number, bandwidth used and session time. See "Information We Automatically Collect from Mobile Devices on Caesars Properties" below for more

information regarding the collection of information regarding your physical location if you are located on one of the Caesars Properties.

Information We Automatically Collect from Mobile Devices on Caesars Properties. If you have a mobile device, are located on one of our properties, and have your Wi-Fi or Bluetooth functionality enabled, we may collect information concerning your mobile device, including the type of device, device ID, and the precise physical location of your device within and around the Caesars Properties (including geolocation and beacon-based location), for analytics and non-marketing related purposes, such as enabling us to understand our customers' preferences and use of our properties, including general traffic patterns. With your consent, we might also use your location information for marketing purposes, such as to provide you with real-time offers and personalized promotions. If you do not want information concerning your precise location to be collected on Caesars Properties, you may adjust your mobile device location sharing settings and disable the Wi-Fi and Bluetooth functionality in your mobile device settings.

Other Information We Collect Relating to Your Gaming and Purchase History and Other Interactions with Us. When you use any of our gaming services or make a purchase at any of our properties, we may collect transactional information about these activities and store it with your customer account. We may use this information to determine your Caesars Rewards tier level (if you are a Caesars Rewards member) and to make predictions about your preferences, and interests, future spending and gaming activity. When located on one of our properties, you also may be videotaped or photographed in connection with a security incident or for other surveillance purposes.

* * *

SECURITY

We maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control. With regard to information that you transfer to us through one of our websites or mobile apps, please be aware that no data transmission over the Internet or a wireless network can be guaranteed to be 100% secure. As a result, Caesars cannot guarantee or warrant the security of any information you transmit on or through a website or mobile app, and you do so at your own risk.

240. These representations were misleading because, among other things, Caesars did not "maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control."

241. The Privacy Policy also contained material omissions because it failed to disclose that Caesars' data security practices had significant shortfalls regarding its data systems that held consumers' PII.

242. Plaintiffs and Class Members provided their PII to Caesars with the reasonable expectation and mutual understanding that Caesars would take reasonable steps to secure the PII from theft. Caesars failed to do so, in violation of its Privacy Policy and other legal duties discussed below.

E. Caesars Knew or Should Have Known it Faced a Serious Threat from and was a Likely Target of Cyber Criminals

243. The type of PII collected by the hospitality and accommodation industry, makes it particularly appealing to cyber criminals.

244. Trustwave's "2018 Global Security Report" listed hospitality as one of the top three industries most vulnerable to payment card breaches.[30] Other estimates project that hotels are the targets of around 20% of all cyberattacks.[31]

245. In its 2018 Data Breach Investigations Report, Verizon noted that 15% of all data breaches occurring in 2017 involved the accommodation and food services industry.[32] The report noted that there were 338 breaches in the accommodation industry in 2017 alone, including at many of the major hotel brands.[33]

246. In recent years, Choice Hotels, Hard Rock Hotel, Hilton, Hyatt, Kimpton, Marriott, Millennium, Omni, Radisson, Starwood, and Wyndham, among others, have all experienced data

[30] *See* Lena Combs & Joshua Davis, *Why Cybersecurity Matters*, Hotel Management (Oct. 17, 2019, 10:40 AM), https://www.hotelmanagement.net/tech/why-cybersecurity-matters.

[31] *Id.*

[32] *See Verizon 2018 Data Breach Investigations Report*, 11th Ed., at pp. 5, 25, 27, *available at* https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf (last visited July 26, 2024).

[33] *Id.*

breach incidents.[34]

247. "Such unfortunate trends should not come as much of a surprise since hotels are hotbeds of sensitive information. Their data is spread out across porous digital systems…."[35]

248. While hospitality companies have fewer transactions than retail organizations—and thus have data on fewer customers to steal—they collect substantially more valuable and varied personal data for each of their guests. This rich personal data is invaluable to cybercriminals. They can use this data to better impersonate each breached customer, leading to additional identity theft and social engineering attacks. By enabling further attacks, breaching a hotel provides cybercriminals much more value than breaching a company in almost any other industry.[36]

249. The high risk of data breaches in the hotel industry was widely known throughout the field, including to Caesars.

250. Indeed, Caesars identified in its December 31, 2022 Form 10-K that cyberattacks were a significant risk factor that it faced, noting "Compromises of our information systems or unauthorized access to confidential information or our customers' personal information could materially harm our reputation and business."[37]

251. Thus, Caesars was clearly aware of the high risk of data intrusions and the magnitude of the harm that could result from a breach. Despite the known risks, Caesars failed to adopt reasonable safeguards to protect Class Members' PII.

---

[34] *See Timeline: The Growing Number of Hotel Data Breaches*, CoStar.com (April 7, 2020, 10:50 AM), *available at* https://www.costar.com/article/139958097 (last visited Sept. 27, 2023).

[35] *See* Combs, *supra* n. 30.

[36] Nirmal Kumar, *Cybersecurity in Hospitality: An Unsolvable Problem?*, HospitalityBiz (June 27, 2018) (now removed), https://web.archive.org/web/20211017182154/http:/www.hospitalitybizindia.com/detailNews.aspx?aid=28970&sid=42; *The challenges of hospitality cybersecurity: An unsolved problem?*, Deccan Chronicle (Aug. 23, 2018), https://www.deccanchronicle.com/technology/in-other-news/230818/the-challenges-of-hospitality-cybersecurity-an-unsolved-problem.html; *Cybersecurity in hospitality—a growing issue?*, CyberSmart (Mar. 23, 2021), https://cybersmart.com/2021/03/cybersecurity-in-hospitality-a-growing-issue/.

[37] *See* Caesars Entertainment, Inc. Form 10-K for the year ended Dec. 31, 2022, *supra* n. 13.

F. Caesars Failed to Comply with Established Cybersecurity Frameworks and Industry Standards.

252. The FTC has promulgated various guides for businesses, which highlight the importance of implementing reasonable and adequate data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[38]

253. In 2016, the FTC updated its publication titled *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[39] The guidelines noted that:

(a) Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it";

(b) Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

(c) Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

(d) Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

(e) Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.

254. In another publication, the FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require

[38] *See Start With Security: A Guide for Business*, Federal Trade Commission, June 2015, https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited July 26, 2024).

[39] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission, Oct. 2016, https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited July 26, 2024).

complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[40]

255. The FTC has brought many enforcement actions against businesses for failing to adequately protect customer data.

256. Importantly for current purposes, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

257. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

258. In its 2019 Privacy & Data Security Update, the FTC noted that "[s]ince 2002, the FTC has brought more than 70 cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data."[41]

259. In this case, Caesars was fully aware of its obligation to use reasonable and adequate measures to protect consumers' PII, acknowledging as much in its Privacy Policy. Caesars also knew it was a ripe target for hackers. But despite understanding the risks and consequences of inadequate data security, upon information and belief, Caesars failed to comply with FTC data security obligations.

260. Caesars' failure to adopt reasonable safeguards to protect PII constitutes an unfair act or practice under Section 5 of the FTC Act, 15 U.S.C. § 45.

261. Similarly, the National Institute of Standards and Technology (NIST) provides

---

[40] *See Start With Security: A Guide for Business*, *supra* n. 38.

[41] *See Privacy & Data Security Update: 2019*, Federal Trade Commission, 2020, *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf (last visited July 26, 2024).

basic network security guidance enumerating steps to take to avoid cybersecurity vulnerabilities.[42] The NIST guidelines provide valuable insights and best practices to protect network systems and customer data.

262. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.[43]

263. Further, cyber security experts have promulgated a series of best practices that should be implemented by hotels, including the following:

(a) Installing appropriate malware detection software;

(b) Monitoring and limiting network ports;

(c) Protecting web browsers and email management systems;

(d) Setting up network systems such as firewalls, switches and routers;

(e) Monitoring and protection of physical security systems; and

(f) Training hotel staff regarding critical points.[44]

264. Beyond its statement that the Data Breach was the result of a "social engineering attack on an outsourced IT support vendor," Caesars has concealed the specific details of how Scattered Spider exploited vulnerabilities in Caesars' data systems.

265. Nevertheless, shortly after the Data Breach, the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity

---

[42] *See Framework for Improving Critical Infrastructure Cybersecurity*, Nat'l Inst. of Standards and Tech. (April 16, 2018), Appendix A, Table 2, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. A new framework was published in 2024, after the Data Breach. *See* CSF 2.0 Resource Center, *available at* https://www.nist.gov/cyberframework (last accessed July 28, 2024).

[43] *Id*. at Table 2 pg. 26-43.

[44] *See How to Work on Hotel Cyber Security*, Open Data Security (July 23, 2019), *available at* https://opendatasecurity.io/how-to-work-on-hotel-cyber-security/.

Advisory (CSA) in response to Scattered Spider actions.[45] The CSA detailed Scattered Spider's social engineering techniques including "phishing, push bombing, and subscriber identity module (SIM) swap attacks, to obtain credentials, install remote access tools, and/or bypass multi-factor authentication (MFA)" and provided specific mitigation techniques to protect against them.[46] Upon information and belief, Scattered Spider used one or more of these social engineering techniques to access and download the Caesars' Rewards database.

266. To mitigate against Scattered Spider's social engineering techniques, CISA and the FBI recommend:[47]

(a) Auditing remote access tools on a network to identify currently used and/or authorized software.

(b) Reviewing logs for execution of remote access software to detect abnormal use of programs running as a portable executable.

(c) Requiring authorized remote access solutions to be used only from within the network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).

(d) Implementing FIDO/WebAuthn authentication or Public Key Infrastructure (PKI)-based MFA. These MFA implementations are resistant to phishing and not suspectable to push bombing or SIM swap attacks, which are techniques known to be used by Scattered Spider actors.

(e) Requiring phishing-resistant multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.

267. Caesars was, or should have been, aware of and implemented these mitigation

[45] Cybersecurity Advisory Scattered Spider (AA23-320A), *supra* n. 18.

[46] *Id.*

[47] *Id.*

techniques prior to Data Breach as they were publicly available and appeared in CISA's publications such as its *Guide to Securing Remote Access Software*,[48] *Implementing Phishing-Resistant MFA*,[49] and *Cross-Sector Cybersecurity Performance Goals*.[50] Upon information and belief, it did not implement one of more of these techniques as evidenced by the Data Breach.

268. Caesars' failure to protect Plaintiffs and Class Members' PII illustrates Caesars' failure to adhere to the spirit and letter of the FTC guidelines, NIST guidance, and industry best practices.

G. Plaintiffs and Class Members Suffered Damages

269. Caesars' failure to keep the PII of Plaintiffs and Class Members secure has severe ramifications. Plaintiffs and Class Members face a high risk of misuse of their PII from the Data Breach. Upon information and belief, the hackers stole PII from Caesars with the specific intent to use it for illicit purposes and/or sell it to others to be misused. And the hackers have carried out this intent by using the data to demand a ransom payment from the Defendant—which Caesars paid in part.

1. Actual and Attempted Fraud and Mitigation Efforts

270. Plaintiffs' PII is now in the hands of Scattered Spider, described by Microsoft as "one of the most dangerous financial criminal groups."[51] Scattered Spider's criminal activity is so prolific that following the Data Breach, the FBI and CISA released published the CSA to

[48] CISA, Guide to Securing Remote Access Software (June 6, 2023), https://www.cisa.gov/sites/default/files/2023-06/Guide%20to%20Securing%20Remote%20Access%20Software_clean%20Final_508c.pdf.

[49] CISA, Implementing Phishing-Resistant MFA (Oct. 2022), https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[50] CISA, Cross-Sector Cybersecurity Performance Goals, v1.01 (March 2023), https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.

[51] *Microsoft Warns as Scattered Spider Expands from SIM Swaps to Ransomware*, The Hacker News (Oct. 26, 2023), https://thehackernews.com/2023/10/microsoft-warns-as-scattered-spider.html.

"encourage critical infrastructure organizations to implement the recommendations in the Mitigations section of this CSA *to reduce the likelihood and impact of a cyberattack by Scattered Spider actors*."[52]

271. As noted in Section, II.A., PII of the Plaintiffs and Class Members have already been misused and exploited for fraud. In addition, Scattered Spider is known to have exfiltrated data to "multiple sites included U.S.-based data centers and MEGA.NZ."[53]

272. Plaintiffs and Class Members have already incurred or will incur out of pocket costs as a result of the Data Breach. As an example, Plaintiff Gill has spent $400 for a one-year subscription for identify protection services.

273. Plaintiffs' PII has already been found on the Dark Web and Plaintiffs' experience measurable increases in targeted identity theft attempts.

274. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial and other accounts for fraud, researching and disputing suspicious or fraudulent activity, obtaining and reviewing credit reports, placing credit freezes on their credit profiles, dealing with spam and phishing emails, text messages, and phone calls, and reviewing their financial affairs more closely than they otherwise would have, among other things. These efforts are burdensome and time-consuming and would not have been necessary but for Caesars' data security shortfalls.

275. Even in instances where a Class Member is reimbursed for a financial loss due to fraud, that does not make the individual whole again because there is typically significant time and effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to fraud and identity theft.[54]

---

[52] Cybersecurity Advisory Scattered Spider (AA23-320A), *supra* n. 18.

[53] *Id.*

[54] *See Victims of Identity Theft*, U.S. Dept. of Justice (Nov. 13, 2017), *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 29, 2024).

2. Loss of Value of PII

276. Plaintiffs and Class Members have also suffered a "loss of value of PII."

277. A robust market exists for stolen PII, which is sold and distributed on the dark web and through illicit criminal networks at specific, identifiable prices. Cybercriminals routinely market stolen PII online, making the information widely available to criminals across the world.

278. For example, stolen driver's license numbers can be sold for between $10 and $35 each.[55]

279. Stolen PII is a valuable commodity to identity thieves. The purpose of stealing large blocks of PII, is to use it for illicit purposes or to sell it and profit from other criminals who buy the data and misuse it.

280. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[56] The Information Commissioner's Office in the European Union, when investigating a hotel data breach at Marriott, noted that "[p]ersonal data has a real value so organi[z]ations have a legal duty to ensure its security."[57]

281. Nevada law, too, acknowledges that personal information has intrinsic monetary value. Specifically, Nev. Rev. Stat. § 597.810 provides for statutory damages of $750 for

---

[55] *See* Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec, 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; *How Cybercriminals Make Money*, Keeper, https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html (last visited July 26, 2024).

[56] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice (Feb. 10, 2020), *available at* https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited July 26, 2024).

[57] *See Intention to Fine Marriott International, Inc More Than £99 Million Under GDPR for Data Breach*, ICO News (July 9, 2019), *available at* https://edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-marriott-international-inc-more-ps99-million_en (last visited July 29, 2024).

unauthorized commercial use of a person's name, voice photograph, or likeness by companies conducting business in Nevada.

282. The value of personal information is increasingly evident in our digital economy. Many companies, including Caesars, collect personal information for purposes of data analytics and marketing. Caesars recognizes the value of personal information, collects it to better target customers to increase its profits, and shares it with third parties for similar purposes, discussed above.

283. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[58]

284. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not from a price at which consumers themselves seek to sell it, but rather from the economic benefit consumers derive from being able to use it. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII leads to a loss of the value of the PII.

285. Beyond the immediate risk of actual harm, consumer victims of data breaches also lose the ability to negotiate sharing their PII for services, as their PII has value, and they have been deprived of that negotiated value because it was shared with an unauthorized third party without their consent. As a result, their PII may be used in the future (and, for several Plaintiffs, already has been used) for unauthorized purposes because of this Data Breach.[59]

---

[58] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets*, 15 Rich. J. L. & Tech. 11, 14 (2009).

[59] *See, e.g.,* James K. Wilcox, *Internet Providers Funded Campaign Yielding Millions of Fake Net Neutrality Comments, New York State Says*, Consumer Reports (May 6, 2021),

3. Benefit of Bargain Damages

286. Plaintiffs and Class Members also suffered "benefit of the bargain" damages.

287. Plaintiffs overpaid for Caesars' services that should have been – but were not – accompanied by adequate data security. One component of the cost of Class Members' use of Caesars' services was the implicit promise Caesars made to protect Class Members' PII.

288. Part of the price consumers paid to Caesars was intended to be used to provide adequate data security. Caesars did not do so. Thus, consumers did not get what they paid for.

289. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those that do not, and vice versa. Indeed, if consumers did not value data security and privacy, Caesars would have no reason to tout its data security efforts in its Privacy Policy.

290. Had consumers known the truth about Caesars' deficient data security practices, they would not have stayed at Caesars properties or would have paid less than they did for their rooms.

291. Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for data security safeguards they expected but did not receive.

292. Plaintiffs and Class Members are entitled to monetary compensation for the various types of damages discussed above.

293. They are also entitled to payment for a robust set of identity protection services, including credit monitoring. Such services are reasonable and necessary here. The stolen PII is historical in nature and can be used for identity theft and other types of financial fraud. There is no question that the PII was taken by sophisticated cybercriminals, increasing the risks to Class Members.

---

https://www.consumerreports.org/electronics/net-neutrality/internet-providers-campaign-fake-net-neutrality-comments (noting how "lead generators" used information stolen from data breaches to create comments purportedly from those individuals victimized in the data breach supporting the termination of net neutrality, without obtaining consent or approval to make those comments).

294. Although Caesars offered in its public statements to provide credit monitoring to its loyalty program members, it has only agreed to provide that service for 24 months. This is entirely insufficient to protect Plaintiffs and Class Members from the consequences of identity theft, which are serious and long-lasting. Experts recommend that data breach victims obtain identity protection services for many years after a data breach. Additionally, there is a benefit to early detection and monitoring. Annual subscriptions for comprehensive identity protection services that include three-bureau credit monitoring, alerts on credit inquiries and new account openings, fraud resolution services, dark web monitoring, and identity theft insurance range from $219 to $329 per year. [60] Caesars must provide monetary compensation to Class Members to pay for these services for their lifetimes.

H. Criminals Will Continue to Use Class Members' Stolen PII for Years

295. The risk of fraud following a data breach like this one persists for years. Identity thieves often hold stolen data for months or years before using it, to avoid detection and maximize profits. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because data is often broken into smaller batches when sold or re-sold to appeal to different types of buyers. In addition, stolen data may be distributed through off-line criminal networks and syndicated to be used for crime near where the victim resides.

296. According to a Government Accountability Office Report, the threat of future identity theft lingers for a substantial period of time after a data breach given the time lag between when information is stolen and when it is used:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure

[60] *See* Robert McMillan & Deepa Seetharaman, *Facebook Finds Hack Was Done By Spammers, Not Foreign State,* The Wall Street Journal (Oct. 17, 2018), *available at* https://www.wsj.com/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869 (last visited July 29, 2024).

> the harm resulting from data breaches cannot necessarily rule out all future harm.[61]

297. Another source, discussing a similar data breach of Caesars' competitor MGM Resorts International, stated: "[A]s with many breaches, malicious actors sometimes wait months or years to tip their hand. . . . This is a great example of how these breaches and their fallout can continue to haunt businesses for quite some time. . . . "[62]

298. Accordingly, Class Members may not see the full extent of identity theft or misuse of their personal information for years to come. They face an ongoing risk and must vigilantly monitor their financial and other accounts indefinitely.

299. Moreover, even after Class Members' PII is misused, it may take months or years for them to become aware of the misuse. This complicates the process of disputing and correcting the misuse of their data.

I. PII Stolen in This Data Breach Can be Combined with Data Acquired Elsewhere to Commit Identity Theft

300. Identity thieves can combine PII stolen in the Data Breach with information gathered from other sources such as public sources or even the consumer's social media accounts, to commit identity theft. Thieves can then use the combined data profile to commit fraud including, among other things, opening new financial accounts or taking out loans in the consumer's name, using the consumer's information to obtain government benefits, filing fraudulent tax returns using the consumer's information and retaining the resulting tax refunds, obtaining a driver's licenses in the consumer's name but with another person's photograph, and giving false information to police during an arrest.

---

[61] *See Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, United States Government Accountability Office (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited July 19, 2024).

[62] *See* Doug Olenick, *MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine (Feb. 20, 2020), *available at* https://www.scmagazine.com/news/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers (last visited July 29, 2024).

301. A federal district court has explained the process as follows:

> The threat of identity theft is exacerbated by what hackers refer to as "fullz packages." A fullz package is a dossier that compiles information about a victim from a variety of legal and illegal sources. Hackers can take information obtained in one data breach and cross-reference it against information obtained in other hacks and data breaches. So, for example, if a hacker obtains a victim's . . . health information from UnityPoint, the hacker can combine it with the same victim's Social Security number and phone number from a different data breach. This allows the hacker to compile a full record of information about the individual, which the hacker then sells to others as a package.

Fox v. Iowa Health Sys., 399 F. Supp. 3d 780, 789 (W.D. Wis. 2019).

302. Thieves can also use PII from the Data Breach, alone or in combination with other information about the consumer, to send highly targeted spear-phishing emails to the consumer to obtain more sensitive information. Spear phishing involves sending emails that look legitimate and are accompanied by correct personal and other information about the individual. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Bank of America, Amazon, or even a government entity), the individual provides sensitive information requested in the email. This could include login credentials, account numbers, or various other types of information.

303. Identity thieves can also use PII from the Data Breach in a "SIM swapping" attack to take control of consumers' phone numbers, allowing them to bypass 2-factor authentication to access the consumer's most sensitive accounts. In other words, fraudsters can use breached PII to convince the consumer's mobile phone carrier to port-over the person's mobile phone number to a phone that the hacker controls. A journalist discussing a similar Data Breach of Caesars' competitor MGM described this scheme as follows:

> Exposed phone numbers create an additional risk: SIM swapping. In these scams, criminals use the data they've gathered about a potential victim to convince wireless carriers to move a number to a different phone. The goal is to intercept two-factor authentication codes that are delivered by SMS.[63]

[63] *See* Lee Matthews, *For Sale: Hacked Data On 142 Million MGM Hotel Guests*, Forbes (July 14, 2020), *available at* https://www.forbes.com/sites/leemathews/2020/07/14/mgm-142-million-guests-hacked/?sh=1ca9d7125294 (last visited July 19, 2024).

J. Plaintiffs and Class Members are Entitled to Injunctive Relief

304. Caesars acted on grounds that apply generally to the Class as a whole. Thus, injunctive relief is appropriate on a class-wide basis.

305. Plaintiffs and Class Members are entitled to injunctive relief requiring Caesars to, among other things:

(a) Strengthen its technical and administrative information security controls and adequately fund them for several years;

(b) Submit to regular, independent System and Organization Controls 2 ("SOC 2") Type 2 audits of its enterprise data networks and all security-relevant systems, with scoping and assertion statement established by an independent assessor;

(c) Promptly implement all remediation measures recommended by the SOC 2, Type 2 assessor and any other forensic analysis or incident response entities retained to address the Data Breach;

(d) Implement tokenization or column-level encryption of sensitive PII in all databases;

(e) Delete all PII from non-production database environments;

(f) Appoint an independent, qualified cyber security professional to ensure Caesars compliance with the injunctive relief ordered by the Court, which cost will be borne completely by Caesars.

306. These measures are necessary to guard against future data breaches at Caesars involving Class Members' PII that Caesars continues to retain.

VI. CLASS ACTION ALLEGATIONS

307. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and (c)(4).

308. Plaintiffs seek certification of the following nationwide class:

Nationwide Class: All persons residing in the United States whose PII was accessed in the Data Breach.

309. The Nationwide Class asserts claims against Caesars for Negligence (Count I), Breach of Implied Contract (Count II), Unjust Enrichment (Count III), and violation of the Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 (Count IV).

310. Under the Restatement (Second) of Conflict of Laws §§ 145 and 188, adopted by Nevada courts and applies to the facts here, Nevada substantive law controls the common law tort and contract-based claims of Plaintiffs, regardless of Plaintiffs' state of residency.

311. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, may be applied on a nationwide basis because Caesars' unlawful conduct was centered in Nevada.

312. In addition, or in the alternative, Plaintiffs also seek certification of statewide subclasses under California, Illinois, Indiana, Minnesota, New York, Pennsylvania, Texas, and Virginia law:

> **California Subclass**: All residents of California whose PII was accessed in the Data Breach. Proposed representatives for the California Subclass are Plaintiffs Gill, Hylton, and Rodriguez.
>
> **Illinois Subclass:** All residents of Illinois whose PII was accessed in the Data Breach. Proposed representatives for the Illinois Subclass are Plaintiffs Elvidge, Popp, Gedwill, L. McNichols, T. McNichols, Stacy, and Cherveny.
>
> **Indiana Subclass:** All residents of Indiana whose PII was accessed in the Data Breach. The proposed representative for the Indiana Subclass is Plaintiff Martin.
>
> **Minnesota Subclass:** All residents of Minnesota whose PII was accessed in the Data Breach. Proposed representatives for the Minnesota Subclass are Plaintiffs C. Rubner and W. Rubner.
>
> **New York Subclass:** All residents of New York whose PII was accessed in the Data Breach. Proposed representatives for the New York Subclass are Plaintiffs Brewster and Dwek.
>
> **Pennsylvania Subclass:** All residents of Pennsylvania whose PII was accessed in the Data Breach. Proposed representatives for the Pennsylvania Subclass are Plaintiffs Blair-Smith and Katz.
>
> **Texas Subclass:** All residents of Texas whose PII was accessed in the Data Breach. The proposed representative for the Texas Subclass is Plaintiff Huddleston.
>
> **Virginia Subclass:** All residents of Virginia whose PII was accessed in the Data

Breach. The proposed representative for the Virginia Subclass is Plaintiff Lackey.

313. The statewide subclasses assert statutory claims for violations of The California Unfair Competition Law (UCL), Cal. Bus. & Prof. Code §§ 17200, *et seq.*, (Count V); The California Consumers Legal Remedies Act (CLRA), Cal. Civ. Code §§ 1750, *et seq.* (Count VI); The California Customer Records Act (CCRA), Cal. Civ. Code §§ 1798.80, *et seq.* (Count VII); Illinois Personal Information Protection Act, 815 ILCS §§ 530/10(a), *et seq.* (Count VIII); Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, *et seq.* and 815 ILCS 530/45(a) (Count IX); Illinois Uniform Deceptive Trade Practices Act, ILCS §§ 510/1, *et seq.* (Count X); Indiana Deceptive Consumer Sales Act Ind. Code §§ 24-5-0.5-1, *et seq.* (Count XI); Minnesota Consumer Fraud Act, Minn. Stat. § 325F.68, *et seq.* and Minn. Stat. § 8.31, *et seq.* (Count XII); Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.43, *et seq.* (Count XIII); New York General Business Law, N.Y. Gen. Bus. Law § 349 (Count XIV); Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Cons. stat. §§ 201-2 & 201-3, *et seq*. Count (XV); Texas Deceptive Trade Practices-Consumer Protection Act, Texas Bus. & Com. Code § 17.41, *et seq.* (Count XVI); The Virginia Personal Information Breach Notification Act, Va. Code. Ann. §§ 18.2-186.6, *et seq*. (Count XVII), and the Virginia Consumer Protection Act. Va. Code Ann. §§ 59.1-196, *et seq*. (Count XVIII).

314. Excluded from the Nationwide Class and all Subclasses (collectively the "Class") are Defendant's executive officers and directors, the judges to whom this case is assigned, their immediate family members, and court room staff.

315. Plaintiffs reserve the right to amend the definitions of the Classes after having an opportunity to conduct discovery.

316. ***Numerosity: Fed. R. Civ. P. 23(a)(1).*** Upon information and belief, the Nationwide Class and statewide Subclass are each so numerous that joinder of all members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, the class size can be determined by information available in Caesars' records, which will be a subject of discovery. On information and belief, there are millions of Class Members in the Nationwide

Class, and at least thousands of Class Members in each state Subclass.

317. ***Commonality: Fed. R. Civ. P. 23(a)(2).*** There are many "questions of law or fact" common to the Class for purposes of Rule 23(a)(2), including but not limited to:

(a) Whether Caesars' data security systems prior to the Data Breach complied with applicable data security laws, regulations, industry standards, and other relevant requirements;

(b) Whether Caesars owed a duty to Plaintiffs and Class Members to safeguard their PII;

(c) Whether Caesars breached its duty to Plaintiffs and Class Members to safeguard their PII;

(d) Whether Caesars knew or should have known that its data security systems were deficient prior to the Data Breach;

(e) Whether Caesars detected the Data Breach in a timely manner;

(f) Whether Caesars had a contractual obligation, based on its Privacy Policy or otherwise, to adopt reasonable data security measures;

(g) Whether Caesars failed to provide timely and adequate notice of the Data Breach to Class Members;

(h) Whether Caesars' conduct constituted violations of state consumer protection statutes and state data security and breach notification statutes;

(i) Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of the Data Breach; and

(j) Whether Plaintiffs and Class Members are entitled to injunctive relief.

318. ***Typicality: Fed. R. Civ. P. 23(a)(3).*** Typicality is satisfied because the claims of Plaintiffs and all Class Members derive from the same operative facts. Plaintiffs and Class Members all had their PII stolen in the Data Breach. Plaintiffs and Class Members have the same basic legal claims against Caesars.

319. ***Adequacy of Representation: Fed R. Civ. P. 23(a)(4).*** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have retained competent counsel who are highly experienced in data breach class actions and other complex litigation. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Class. Plaintiffs' counsel have the financial and personnel resources to litigate this matter through all phases of pretrial litigation, trial, and any necessary appeals. Neither Plaintiffs nor their counsel have any

interests that are contrary to, or conflict with, those of the Class.

320. ***Predominance: Fed. R. Civ. P. 23(b)(3).*** Caesars has engaged in a common course of conduct toward all Class Members. The common issues identified above arising from Caesars' conduct predominate over any issues affecting only individual Class Members. The common issues hinge upon Caesars' conduct rather than that of any individual plaintiff or class member. Adjudication of the common issues in a single action has important and desirable advantages that will lead to judicial economy.

321. ***Superiority: Fed. R. Civ. P. 23(b)(3).*** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law of fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would find that the cost of litigating their individual claims is prohibitively high and they would therefore have no realistic means to a remedy on an individual non-class basis. The litigation of separate actions by consumers would create a risk of inconsistent or varying adjudications, which could establish incompatible standards of conduct for Caesars. In contrast, conducting this action on a class-wide basis presents fewer management difficulties, conserves judicial and party resources, and pursues the rights of all Class Members in a single proceeding.

322. ***Injunctive Relief: Fed. R. Civ. P. 23(b)(2).*** Caesars acted on grounds that apply generally to the Class as a whole. Caesars continues to retain Class Members' PII, which is subject to potential future data breaches in Caesars' hands. Injunctive relief is appropriate on a class-wide basis.

323. ***Certification of Issues: Fed. R. Civ. P. 23(c)(4).*** In the alternative, Plaintiffs request that the Court certify the case to proceed as a class action on particular issues, as described herein, which would substantially advance the litigation to trial.

/ / /

/ / /

VII. CAUSES OF ACTION

CLAIM FOR RELIEF I
NEGLIGENCE
Brought by all Plaintiffs on behalf of the Nationwide Class or, in the Alternative, Negligence According to the Applicable State Subclasses

324. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

325. As a condition of receiving Caesars' services, Plaintiffs and all Class Members were obligated to provide Caesars with their PII.

326. Plaintiffs and Class Members entrusted their PII to Caesars with the understanding that Caesars would take reasonable measures to safeguard their PII.

327. Caesars had knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could face if their PII was stolen in a data breach.

328. Caesars had a duty to exercise reasonable care in safeguarding, securing, and protecting Class Members' PII. This duty included, among other things, designing, maintaining, and testing Caesars' data security procedures to ensure that the PII was adequately protected, that cloud-based safeguards were adequately implemented, and that employees tasked with maintaining PII were adequately trained on cyber security measures.

329. Caesars' duty of care arose from, among other things:

- the special relationship that existed between Caesars and its customers because, *e.g.*, Caesars was in an exclusive position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;
- Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures;
- Caesars' representations in its Privacy Policy;
- General common law duties to adopt reasonable data security measures to protect customer PII and to act as a reasonable and prudent person under the same or similar

circumstances would act; and

330. State statutes requiring reasonable data security measures, including but not limited to Nev. Rev. Stat. § 603A.210, which states that businesses possessing personal information of Nevada residents "shall implement and maintain reasonable security measures to protect those records from authorized access."

331. Caesars was subject to an "independent duty," untethered to any express contract between Caesars and Class Members. Sources of the independent duty are included in the list above.

332. Caesars' violation of the FTC Act and state data security statutes constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a group to which Plaintiffs belong and to prevent the type of harm that resulted from the Data Breach.

333. Plaintiffs and Class Members were the foreseeable victims of Caesars' inadequate data security practices. Caesars knew that a breach of its systems could cause harm to Plaintiffs and Class Members.

334. Caesars' conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Caesars' misconduct included its failure to adequately restrict access to its cloud server that held consumers' PII.

335. Caesars knew or should have known of the inherent risks in collecting and storing PII, the importance of providing adequate data security, and the frequent cyberattacks aimed at the hotel industry.

336. Plaintiffs and Class Members had no ability to protect their PII once it was in Caesars' possession and control. Caesars was in an exclusive position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

337. Caesars, through its actions and inactions, breached its duties owed to Plaintiffs and Class Members by failing to exercise reasonable care in safeguarding their PII while it was in Caesars' possession and control.

338. Caesars inadequately safeguarded consumers' PII in deviation of standard industry rules, regulations, and best practices at the time of the Data Breach.

339. But for Caesars' breach of duties, consumers' PII would not have been stolen by a computer hacker.

340. There is a temporal and close causal connection between Caesars' failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs and Class Members.

341. As a result of Caesars' negligence, Plaintiffs and Class Members suffered and will continue to suffer the various types of damages alleged herein—including, but not limited to, significant risk of substantial and immediate future harm, identity theft and fraud, additional time, resources, and money spent on mitigation efforts, increased phishing and attempts at fraud, and further loss of value of personal information.

342. Due to Defendant's conduct, Plaintiffs and Class Members are also entitled to identity protection and credit monitoring. Identity protection and credit monitoring is reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Class Members. There is no question that this PII was taken by sophisticated cybercriminals increasing the risks to the Class Members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring. Some experts recommend that data breach victims obtain credit monitoring services for many years after a data breach. Annual subscriptions for comprehensive credit monitoring plans that include inquiry alerts, credit locks, and identity theft insurance range from $219 to $329 per year.[64]

343. Plaintiffs and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth above.

/ / /

/ / /

[64] McMillan, *supra* n. 60.

CLAIM FOR RELIEF II
BREACH OF IMPLIED CONTRACT
Brought by All Plaintiffs on behalf of the Nationwide Class

344. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

345. When Plaintiffs and Class Members provided consideration and PII to Caesars in exchange for Caesars' services, they entered into implied contracts with Caesars under which Caesars agreed to adopt reasonable steps to protect their PII.

346. Caesars solicited and invited Plaintiffs and Class Members to purchase its services. As part of that process, Plaintiffs and Class Members were required to provide their PII.

347. When entering into the implied contracts, Plaintiffs and Class Members reasonably believed and expected that Caesars would implement reasonable and adequate data security measures and that Caesars' data security practices complied with relevant laws, regulations, and industry standards. Caesars knew or reasonably should have known that Plaintiffs and Class Members held this belief and expectation.

348. When entering into the implied contracts, Caesars impliedly promised to adopt reasonable data security measures. Caesars required consumers to provide their PII during the reservation and/or check-in process. In doing so, Caesars made implied or implicit promises that its data security practices were reasonably sufficient to protect consumers' PII. By virtue of accepting Plaintiffs' PII during the reservation and check-in process, Caesars implicitly represented that its data security processes were reasonably sufficient to safeguard the PII.

349. Caesars' conduct in requiring consumers to provide PII as a prerequisite to the use of Caesars' services illustrates Caesars' intent to be bound by an implied promise to adopt reasonable data security measures.

350. Plaintiffs and Class Members would not have provided their PII to Caesars in the absence of Caesars' implied promise to keep the PII reasonably secure.

351. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Caesars. They provided consideration and their PII to Caesars in exchange for

Caesars' services and its implied promise to adopt reasonable data security safeguards.

352. Caesars breached its implied contracts with Plaintiffs and Class Members by failing to implement reasonable data security measures.

353. As a result of Caesars' conduct, Plaintiffs and Class Members have suffered, and continue to suffer, legally cognizable damages arising from the Data Breach as set forth above in Section II.A.

354. Plaintiffs and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

CLAIM FOR RELIEF III
UNJUST ENRICHMENT
Brought by All Plaintiffs on behalf of the Nationwide Class

355. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

356. This claim is plead in the alternative to the breach of implied contract claim.

357. Plaintiffs and Class Members conferred monetary benefits on Caesars.

358. In exchange, Plaintiffs and Class Members should have received Caesars' services as well as adequate safeguarding of their PII.

359. Caesars profited from its transactions with Class Members in two ways. First, Caesars received monetary consideration as revenue. Second, Caesars used Class Members' PII for a variety of profit-generating purposes beyond simply providing its services. Caesars used the PII for marketing and other purposes discussed more fully above. Caesars used the PII to generate future stays from consumers and derive future revenues and profit.

360. The money Plaintiffs and Class Members paid to Caesars was intended to be used by Caesars, in part, to fund Caesars' costs of providing reasonable data security.

361. Caesars failed to provide reasonable data security, yet it kept all monies paid by Plaintiffs and Class Members.

362. Caesars knew that Plaintiffs and Class Members conferred monetary and other

benefits on Caesars. Caesars accepted those benefits.

363. Under principles of equity and good conscience, Caesars should not be permitted to retain the full monetary benefit of its transactions with Plaintiffs and Class Members. Caesars failed to adequately secure consumers' PII and, therefore, did not provide the full services that consumers paid for.

364. Caesars acquired consumers' money and PII through inequitable means in that it failed to disclose its inadequate data security practices when entering into transactions with consumers and obtaining their PII.

365. If Plaintiffs and Class Members would have known that Caesars employed inadequate data security safeguards, they would not have agreed to provide Caesars with their PII or required Caesars to increase their security.

366. Class Members have no adequate remedy at law. Caesars continues to retain Class Members' PII while exposing the PII to a risk of future data breaches while in Caesars' possession. Caesars also continues to derive a financial benefit from using Class Members' PII.

367. As a direct and proximate result of Caesars' conduct, Plaintiffs and Class Members have suffered the various types of damages alleged herein.

368. Caesars should be compelled to disgorge into a common fund or constructive trust, for the benefit of Class Members, the proceeds that they unjustly received from Class Members. In the alternative, Caesars should be compelled to refund the amounts that Class Members overpaid for Caesars' services.

CLAIM FOR RELIEF IV
VIOLATION OF THE NEVADA CONSUMER FRAUD ACT
Nev. Rev. Stat. § 41.600
Brought by All Plaintiffs on behalf of the Nationwide Class

369. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

370. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, states:

1. An action may be brought by any person who is a victim of

> consumer fraud.
>
> 2. As used in this section, "consumer fraud" means: . . . (e) A deceptive trade practice as defined in NRS 598.0915 to 598.0925, inclusive.

371. In turn, Nev. Rev. Stat. § 598.0923(2) (a section of the Nevada Deceptive Trade Practices Act) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 2) Fails to disclose a material fact in connection with the sale or lease of goods or services." Caesars violated this provision because it failed to disclose the material fact that its data security practices were deficient and that its cloud server security settings were not adequate to protect consumers' PII. Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the omission. Caesars could and should have made a proper disclosure when accepting hotel reservations, during the check-in process, in the registration for its Caesars Rewards loyalty program, in its Privacy Policy, or by any other means reasonably calculated to inform consumers of its inadequate data security.

372. Also, Nev. Rev. Stat. § 598.0923(3) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 3) Violates a state or federal statute or regulation relating to the sale or lease of . . . services." Caesars violated this provision for several reasons, each of which is an independent predicate act for purposes of violating § 598.0923(3).

373. *First*, Caesars breached a Nevada statute requiring reasonable data security. Specifically, Nev. Rev. Stat. § 603A.210(1) states: "A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain *reasonable security measures* to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." (Emphasis added.) Caesars is a data collector as defined under the

statute at Nev. Rev. Stat. § 603A.030. Caesars failed to implement and maintain reasonable security measures, evidenced by the fact that hackers accessed its cloud server and stole consumers' PII. Caesars' violation of this statute was done knowingly for purposes of Nev. Rev. Stat. § 598.0923(3). Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the violation.

374. *Second*, Caesars breached other state statues as alleged herein. Caesars also violated Nev. Rev. Stat. § 598.0923(2) as alleged in this Count. Caesars knew or should have known that it violated these statutes. Caesars' violation of each of these statutes serves as a separate predicate act for purposes of violating Nev. Rev. Stat. § 598.0923(3).

375. *Third*, Caesars violated the FTC Act, 15 U.S.C. § 45, as alleged above. Caesars knew or should have known that its data security practices were deficient, violated the FTC Act, and that it failed to adhere to the FTC's data security guidance for businesses. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the violation. Caesars' violation of the FTC Act serves as a predicate act for violating Nev. Rev. Stat. § 598.0923(3).

376. Caesars engaged in deceptive or unfair practices by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Class Members.

377. Plaintiffs and Class Members were denied a benefit conferred on them by the Nevada legislature.

378. Nev. Rev. Stat. § 41.600(3) states that if the plaintiff prevails, the court "shall award: (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court deems appropriate; and (c) the claimant's costs in the action and reasonable attorney's fees."

379. As a direct and proximate result of the foregoing, Plaintiffs and Class Members suffered all forms of damages alleged herein in Section II.A. Plaintiffs' harms constitute compensable damages under Nev. Rev. Stat. § 41.600(3).

380. Plaintiffs and Class Members are also entitled to all forms of injunctive relief sought herein.

381. Plaintiffs and Class Members are also entitled to an award of their attorney's fees and costs.

CLAIM FOR RELIEF V
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW (UCL),
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
Brought by California Plaintiffs Gill, Hylton, and Rodriguez
on behalf of the California Subclass

382. The California Plaintiffs (or "Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

383. Caesars and the California Plaintiffs are "persons" as defined by Cal. Bus. & Prof. Code § 17201.

384. The UCL states that "unfair competition shall mean and include any [1] unlawful, unfair or fraudulent business act or practice and [2] unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

385. The first section of the UCL quoted above includes three separate prongs: "unlawful," "unfair," or "fraudulent" practices. Caesars violated each of these prongs by engaging in unlawful, unfair, and fraudulent business acts and practices.

386. Caesars' "unfair" acts and practices include:

387. Caesars failed to implement and maintain reasonable security measures to protect Plaintiffs' and California Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

388. Caesars failed to identify foreseeable security risks, remediate identified security

risks, and sufficiently improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and California Subclass Members, whose PII has been compromised.

389. Caesars' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

390. Caesars' failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of Caesars' grossly inadequate security, consumers could not have reasonably avoided the harms that Caesars caused.

391. Caesars engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

392. Caesars has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law, all as alleged herein.

393. Caesars also engaged in "fraudulent" acts or practices, including but not limited to the following:

394. Caesars omitted and concealed the fact that it did not employ reasonable safeguards to protect consumers' PII. Caesars could and should have made a proper disclosure when accepting hotel reservations, during the check-in process, or by any other means reasonably calculated to inform consumers of the inadequate data security. Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should

have known that its data security was insufficient to guard against those attacks.

395. Caesars also made implied or implicit false representations that its data security practices were sufficient to protect consumers' PII. Caesars required consumers to provide their PII during the reservation and/or check-in process. In doing so, Caesars made implied or implicit representations that its data security practices were sufficient to protect consumers' PII. By virtue of accepting Plaintiffs' PII during the reservation and check-in process, Caesars implicitly represented that its data security procedures were sufficient to safeguard the PII. Those representations were false and misleading.

396. Caesars retained consumers' PII for years after the original hotel stays, much longer than was necessary to achieve the goal of processing the consumers' hotel room rentals. As a result, Caesars amassed an enormous trove of PII. Given the volume and sensitivity of PII within Caesars' database, Caesars knew that it should have taken adequate measures to protect the data. Caesars failed to do so.

397. Caesars' unlawful, unfair, and deceptive acts and practices also included:

398. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

399. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

400. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

401. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

402. Misrepresenting that it would comply with common law and statutory duties

pertaining to the security and privacy of Plaintiffs' and California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

403. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and California Subclass Members' PII;

404. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California's Consumer Records Act, Cal. Civ. Code § 1798.80, *et seq.*, and § 1798.81.5, which was a direct and proximate cause of the Data Breach; and

405. Failing to provide the Notice of Data Breach required by Cal. Civ. Code § 1798.82(d)(1).

406. Caesars' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Caesars' data security and ability to protect the confidentiality of consumers' PII.

407. As a direct and proximate result of Caesars' unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

408. Caesars acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and California Subclass Members' rights.

409. The Plaintiffs and California Subclass members transacted with Caesars in California by, among other things, making hotel reservations from California and paying any

necessary room deposits from California. The California Plaintiffs and California Subclass members were deceived in California when they made reservations from California and were not informed of Caesars' deficient data security practices.

410. The UCL states that an action may be brought by any person who has "suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code §17204. The Plaintiffs and California Subclass members suffered injury in fact and lost money or property as a result of Caesars' unfair competition as set forth herein. This includes, e.g., the loss of value in their breached PII. PII is valuable, which is demonstrated not only by the fact that Caesars requires consumers to provide PII during the reservation and check-in process, but also because Caesars uses PII for its marketing and other purposes. Furthermore, PII stolen from Caesars was marketed on the "dark web." Due to Caesars' misconduct and the resulting Data Breach, hackers took this valuable PII without providing compensation to Plaintiffs and Class Members.

411. Cal. Bus. & Prof. Code §17203 states:

> Any person who engages, has engaged, or proposes to engage in unfair competition may be enjoined in any court of competent jurisdiction. The court may make such orders or judgments . . . as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition, as defined in this chapter, or as may be necessary to restore to any person in interest any money or property, real or personal, which may have been acquired by means of such unfair competition.

412. The Plaintiffs and California Subclass members are entitled to the injunctive relief requested herein to address Caesars' past and future acts of unfair competition.

413. The Plaintiffs and California Subclass members are entitled to a restoration of money or property that was acquired by Caesars' by means of its unfair competition.

414. Plaintiffs and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Caesars' unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

CLAIM FOR RELIEF VI
VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT (CLRA), Cal. Civ. Code §§ 1750, *et seq.*,
Brought by California Plaintiffs Gill, Hylton, and Rodriguez on behalf of the California Subclass

415. The California Plaintiffs (or "Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

416. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

417. Caesars is a "person" as defined by Civil Code §§ 1761(c) and 1770 and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

418. Plaintiffs and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

419. Caesars' acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the California Subclass Members in violation of Civil Code § 1770(a), including by:

- Representing that goods or services have characteristics that they do not have;
- Representing that goods or services are of a particular standard, quality, or grade when they were not;
- Advertising goods or services with intent not to sell them as advertised; and
- Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

420. Caesars' acts and practices resulted in the sale of services that violated Cal. Civil Code § 1770(a).

421. Omissions are actionable under Cal. Civil Code § 1770(a).

422. Caesars' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Caesars' data security and ability to protect the confidentiality of consumers' PII.

423. Had Caesars disclosed to Plaintiffs and California Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, Caesars would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Caesars was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs and California Subclass Members. Caesars accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and California Subclass Members acted reasonably in relying on Caesars' misrepresentations and omissions, the truth of which they could not have discovered.

424. The Plaintiffs and California Subclass members transacted with Caesars in California by, among other things, making hotel reservations from California and paying any necessary room deposits from California. The California Plaintiffs and California Subclass members were deceived in California when they made reservations from California and were not informed of Caesars' deficient data security practices.

425. Cal. Civ. Code § 1780(a) states:

> Any consumer who suffers any damage as a result of the use or employment by any person of a method, act, or practice declared to be unlawful by Section 1770 may bring an action against that person to recover or obtain any of the following:
>
> 1) Actual damages, but in no case shall the total award of damages in a class action be less than one thousand dollars ($1,000).
> 2) An order enjoining the methods, acts, or practices.
> 3) Restitution of property.
> 4) Punitive damages.
> 5) Any other relief that the court deems proper.

426. As a direct and proximate result of Caesars' violations of California Civil Code § 1770, Plaintiffs and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

427. Plaintiffs suffered "damages" and "actual damages" based on the various damages alleged herein.

428. Plaintiffs are entitled to the injunctive relief sought herein to enjoin Caesars' unlawful methods, acts, or practices.

429. Plaintiffs are entitled to "restitution of property," including but not limited to the value of monies they overpaid to Caesars for its services and the value of the PII they provided to Caesars.

430. Plaintiffs are also entitled to punitive damages under Cal. Civ. Code § 1780(a)(4). Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its data security was insufficient to guard against those attacks. Also, given the size of Caesars' database and the sensitivity of the PII therein, Caesars should have taken adequate measures to protect the data. Caesars intentionally failed to encrypt the PII while it was stored on Caesars' server. Also, Caesars intentionally retained consumers' PII for years after their original hotel stays, much longer than was necessary to achieve the goal of processing the consumers' transactions.

431. Cal. Civ. Code § 1780(e) states that the "court shall award court costs and attorney's fees to a prevailing plaintiff in litigation filed pursuant to this section." Plaintiffs are entitled to an award of attorney's fees and costs.

432. Caesars' violations of the CLRA were not the result of a "bona fide error" for

purposes of Cal Civ. Code § 1784. Instead, Caesars acted with knowledge, recklessness, gross negligence, negligence, and/or any other form of actionable misconduct.

433. As a result of Caesars' violations of Cal. Civ. Code § 1770(a), the California Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages of the various types alleged herein.

434. Plaintiffs satisfy all requirements for class action treatment set forth in Cal. Civ Code § 1781(b). As discussed more fully above in the Class Action Allegations section, it is impracticable to bring all members of the California Subclass before the court. The questions of law or fact common to the class are substantially similar for each Class member, and they predominate over any questions affecting individual Class Members. The claims of the Plaintiffs are typical of the claims of the California Subclass. The Plaintiffs will fairly and adequately represent the interests of the California Subclass.

435. Plaintiffs have provided timely notice to Caesars of their claims for damages under the CLRA, in compliance with Cal. Civ. Code § 1782(a). To date, Caesars has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by California Plaintiffs' counsel.

436. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

CLAIM FOR RELIEF VII
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT (CCRA)
Cal. Civ. Code §§ 1798.80, *et seq.*
Brought by California Plaintiffs Gill, Hylton, and Rodriguez on behalf of the California Subclass

437. The California Plaintiffs (or "Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

438. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information [PII] from unauthorized access, destruction, use, modification, or disclosure."

439. Caesars is a business that owns, maintains, and licenses personal information (or "PII"), within the meaning of Cal. Civ. Code §§ 1798.80(a) and 1798.81.5(b), about Plaintiffs and California Subclass Members.

440. Businesses that own or license computerized data that includes PII are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of personal information [PII] that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

441. The CCRA defines owns, licenses, and maintains as follows: "[T]he terms 'own' and 'license' include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term 'maintain' includes personal information that a business maintains but does not own or license.'" Cal. Civ. Code § 1798.81.5(a)(2). Caesars owns, licenses, and/or maintains the PII that was involved in the Data Breach.

442. The CCRA defines personal information as follows: "'Personal information' means either of the following: (A) An individual's first name of first initial and the individual's last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: . . . (ii) Driver's license number, . . . passport number, [or] military identification number . . . ." Cal. Civ. Code § 1798.81.5(d)(1)(A)(ii). The PII stolen in the Data Breach includes personal information that meets this definition. The PII was

unencrypted, evidenced by the fact that it was posted to the dark web in a readable form. Each of the California Plaintiffs provided their PII to Caesars when transacting with Caesars' hotels and casinos.

443. Caesars is a business that owns or licenses computerized data that includes "personal information" [PII] as defined by Cal. Civ. Code § 1798.80.

444. Plaintiffs' and California Subclass Members' PII includes "personal information" as covered by Cal. Civ. Code § 1798.82.

445. Caesars failed to maintain reasonable data security procedures appropriate to the nature of the PII. Accordingly, Caesars violated Cal. Civ. Code § 1798.81.5(b).

446. Because Caesars reasonably believed that Plaintiffs' and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Caesars had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

447. Caesars failed to fully disclose material information about the Data Breach, including the types of PII impacted.

448. By failing to disclose the Data Breach in a timely and accurate manner, Caesars violated Cal. Civ. Code § 1798.82.

449. Caesars also violated Cal. Civ. Code § 1798.82 by not publishing a notice of data breach in the format required by Cal. Civ. Code § 1798.82(d)(1).

450. As a direct and proximate result of Caesars' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, the California Plaintiffs and California Subclass members were "injured" by Caesars' violation of Cal. Civ. Code § 1798.81.5(b) and seek "damages" pursuant to Cal. Civ. Code § 1798.84(b). The California Plaintiffs and California Subclass members were injured in the various ways alleged herein. They seek all monetary and non-monetary relief allowed by the CCRA to compensate for their various types of damages alleged herein.

451. The California Plaintiffs and California Subclass members are also entitled to injunctive relief pursuant to Cal. Civ. Code § 1798.84(e), including but not limited to substantial

improvements to Caesars' data security systems and all other injunctive remedies sought herein.

452. Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

CLAIM FOR RELIEF VIII
VIOLATION OF ILLINOIS PERSONAL INFORMATION PROTECTION ACT
815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*
Brought by Illinois Plaintiffs Elvidge, Popp, Gedwill, L. McNichols, T. McNichols, Stacy, and Cherveny on behalf of the Illinois Subclass

453. The Illinois Plaintiffs ("Plaintiffs" for purposes of this Count), individually and on behalf of the Illinois Subclass, re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

454. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information (for the purpose of this count, "PII"), Caesars is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

455. Caesars is a Data Collector that owns or licenses computerized data that includes PII. Caesars also maintains computerized data that includes PII which Caesars does not own.

456. Plaintiffs' and Illinois Subclass Members' PII includes "personal information" as defined by 815 Ill. Comp. Stat. § 530/5.

457. Caesars is required to give immediate notice of a breach of a security system to owners of PII which Caesars does not own or license, including Plaintiffs and Illinois Subclass Members, pursuant to 815 Ill. Comp. Stat. § 530/10(b).

458. By failing to give immediate notice to Plaintiffs, Caesars violated 815 Ill. Comp. Stat. § 530/10(b).

459. Caesars is required to notify Plaintiffs and Illinois Subclass Members of a breach of its data security system which may have compromised PII which Caesars owns or licenses in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

460. By failing to disclose the Data Breach to Plaintiffs and Illinois Subclass Members

in the most expedient time possible and without unreasonable delay, Caesars violated 815 Ill. Comp. Stat. § 530/10(a).

461. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

462. As a direct and proximate result of Caesars' violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiffs and Illinois Subclass Members suffered damages, as described above.

463. Plaintiffs and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Caesars' willful violations of 815 Ill. Comp. Stat. § 530/10(a), including equitable relief, costs, and attorneys' fees.

CLAIM FOR RELIEF IX
VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 ILCS 505/2, *et seq.* and 815 ILCS 530/45(a)
Brought by Illinois Plaintiffs Elvidge, Popp, Gedwill, L. McNichols, T. McNichols, Stacy, and Cherveny on behalf of the Illinois Subclass

464. The Illinois Plaintiffs (or "Plaintiffs" for purposes of this Count), individually and on behalf of the Illinois Subclass, re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

465. Caesars is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

466. Plaintiffs and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

467. Caesars' conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

468. Caesars' deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the

Data Breach;

- Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), et seq, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;
- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a);
- Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and
- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

469. Caesars' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Caesars' data security and ability to protect the confidentiality of consumers' PII.

470. Caesars intended to mislead Plaintiffs and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

471. The above unfair and deceptive practices and acts by Caesars were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

472. Caesars acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Illinois Subclass Members' rights. Caesars' numerous past data breaches put it on notice that its security and privacy protections were inadequate.

473. As a direct and proximate result of Caesars' unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

474. Plaintiffs and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

CLAIM FOR RELIEF X
VIOLATION OF ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 Ill. Comp. Stat. §§ 510/1, *et seq.*
Brought by Illinois Plaintiffs Elvidge, Popp, Gedwill, L. McNichols, T. McNichols, Stacy, and Cherveny on behalf of the Illinois Subclass

475. The Illinois Plaintiffs (or "Plaintiffs" for purposes of this Count), individually and on behalf of the Illinois Subclass, re-allege and incorporate by reference Paragraphs 1 through 323

as if fully set forth herein.

476. Caesars is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

477. Caesars engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

- Representing that goods or services have characteristics that they do not have;
- Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- Advertising goods or services with intent not to sell them as advertised; and
- Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

478. Caesars' deceptive acts and practices include:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;
- Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;
- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade

Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*;

- Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and
- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

479. Caesars' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Caesars' data security and ability to protect the confidentiality of consumers' PII.

480. The above unfair and deceptive practices and acts by Caesars were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

481. As a direct and proximate result of Caesars' unfair, unlawful, and deceptive trade practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

482. Plaintiffs and Illinois Subclass Members seek all relief allowed by law, including injunctive relief.

/ / /

/ / /

CLAIM FOR RELIEF XI
VIOLATION OF INDIANA DECEPTIVE CONSUMER SALES ACT
Ind. Code §§ 24-5-0.5-1, *et seq.*
Brought by Indiana Plaintiff Martin on behalf of the Indiana Subclass

483. The Indiana Plaintiff ("Plaintiff" for purposes of this Count), individually and on behalf of the Indiana Subclass, re-alleges and incorporates by reference Paragraphs 1 through 323 as if fully set forth herein.

484. Caesars is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

485. Caesars is a "supplier" as defined by § 24-5-0.5-2(a)(3), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(1).

486. Caesars engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

487. Caesars' representations and omissions include both implicit and explicit representations:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;
- Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;
- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties

imposed by the FTC Act, 15 U.S.C. § 45;

- Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and
- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

488. Caesars' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

489. The injury to consumers from Caesars' conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

490. Consumers could not have reasonably avoided injury because Caesars' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Caesars created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

491. Caesars' inadequate data security had no countervailing benefit to consumers or to competition.

492. Caesars' acts and practices were "abusive" for numerous reasons, including:

- Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Caesars' failure to disclose the inadequacies in its data security interfered with consumers' decision- making in a variety of their transactions.
- Because they took unreasonable advantage of consumers' lack of understanding about

the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Caesars' data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

- Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Caesars concerning the state of Caesars security, and because it is functionally impossible for consumers to obtain credit without their PII being in Caesars' systems.
- Because Caesars took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed below.

493. Caesars also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

- Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have;
- Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and
- Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

494. Caesars intended to mislead Plaintiff and Indiana Subclass Members and induced them to rely on its misrepresentations and omissions.

495. Caesars' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Caesars' data security and ability to protect the confidentiality of consumers' PII.

496. Had Caesars disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Caesars would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Caesars was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Caesars accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Caesars' misrepresentations and omissions, the truth of which they could not have discovered.

497. Caesars had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the PII in its possession, and the relevant generally accepted professional standards. This duty arose due to the representations and relationship between Caesars and Plaintiff and the Indiana Subclass as described herein. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Indiana Subclass—and Caesars, because consumers are unable to fully protect their interests with regard to their data and placed trust and confidence in Caesars. Caesars' duty to disclose also arose from its:

- Possession of exclusive knowledge regarding the security of the data in its systems;
- Active concealment of the state of its security; and/or
- Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Indiana Subclass that contradicted these representations.

498. Caesars acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff's and Indiana Subclass Members' rights. Caesars' numerous past data breaches put it on notice that its security and privacy protections were inadequate. Caesars' actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

499. Despite receiving notice, Caesars has not cured its unfair, abusive, and deceptive

acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable. Caesars' conduct includes incurable deceptive acts that Caesars engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5- 0.5- 2(a)(8).

500. As a direct and proximate result of Caesars' uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

501. Caesars' violations present a continuing risk to Plaintiffs and Indiana Subclass Members as well as to the general public.

502. Plaintiff and Indiana Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIM FOR RELIEF XII
VIOLATION OF MINNESOTA CONSUMER FRAUD ACT
Minn. Stat. § 325F.68, *et seq.* and Minn. Stat. § 8.31, *et seq.*
Brought by Minnesota Plaintiffs C. Rubner and W. Rubner on behalf of the Minnesota Subclass

503. The Minnesota Plaintiffs ("Plaintiffs" for purposes of this Count), individually and on behalf of the Minnesota Subclass, re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

504. Caesars, Plaintiffs, and members of the Minnesota Subclass are each a "person" as defined by Minn. Stat. § 325F.68(3).

505. Caesars' goods, services, commodities, and intangibles are "merchandise" as

defined by Minn. Stat. § 325F.68(2).

506. Caesars engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

507. Caesars engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;
- Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

508. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

509. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

510. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

511. Caesars' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Caesars' data security and ability to protect

the confidentiality of consumers' PII.

512. Caesars intended to mislead Plaintiff and Minnesota Subclass Members and induce them to rely on its misrepresentations and omissions.

513. Caesars' fraudulent, misleading, and deceptive practices affected the public interest, including the many Minnesotans affected by the Data Breach.

514. As a direct and proximate result of Caesars' fraudulent, misleading, and deceptive practices, Plaintiffs and Minnesota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

515. Plaintiffs and Minnesota Subclass Members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

CLAIM FOR RELIEF XIII
VIOLATION OF MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT
Minn. Stat. § 325D.43, *et seq.*
Brought by Minnesota Plaintiffs Rubner and W. Rubner on behalf of the Minnesota Subclass

516. The Minnesota Plaintiffs ("Plaintiffs" for purposes of this Count), individually and on behalf of the Minnesota Subclass, re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

517. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, Caesars violated Minn. Stat. § 325D.44, in the following ways:

- Representing that its goods and services had characteristics, uses, and benefits that they did not have;

- Representing that goods and services are of a particular standard or quality when they are of another;
- Advertising goods and services with intent not to sell them as advertised; and
- Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding.

518. Caesars' deceptive practices include:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;
- Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

519. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

520. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

521. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

522. Caesars' representations and omissions were material because they were likely to

deceive reasonable consumers about the adequacy of Caesars' data security and ability to protect the confidentiality of consumers' PII.

523. Caesars intended to mislead Plaintiffs and Minnesota Subclass Members and induce them to rely on its misrepresentations and omissions.

524. Had Caesars disclosed to Plaintiffs and Subclass Members that its data systems were not adequate and, thus, vulnerable to attack, Caesars would have been unable to continue in business and it would have been forced to adopt reasonable and adequate data security measures and comply with the law. Caesars was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs and Subclass Members. Caesars accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Subclass Members acted reasonably in relying on Caesars' misrepresentations and omissions, the truth of which they could not have discovered.

525. Caesars acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Minnesota Subclass Members' rights. Caesars' numerous past data breaches put it on notice that its security and privacy protections were inadequate.

526. As a direct and proximate result of Caesars' deceptive trade practices, Plaintiffs and Minnesota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

527. Plaintiffs and Minnesota Subclass Members seek all relief allowed by law, including injunctive relief and attorneys' fees and costs.

/ / /

/ / /

CLAIM FOR RELIEF XIV
VIOLATION OF NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law § 349
Brought by New York Plaintiffs Brewster and Dwek on behalf of the New York Subclass

528. The New York Plaintiffs ("Plaintiffs" for purposes of this Count), individually and on behalf of the New York Subclass, re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

529. Caesars engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New York Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and New York Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42

U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

- Failing to timely and adequately notify the Plaintiffs and New York Subclass members of the Data Breach;
- Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and New York Subclass members' Private Information; and
- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

530. Caesars' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the New York Subclass members, that their PII was not exposed and misled Plaintiffs and the New York Subclass members into believing they did not need to take actions to secure their identities.

531. Caesars acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs' and New York Subclass members' rights.

532. Caesars' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

533. The above deceptive and unlawful practices and acts by Caesars caused substantial injury to Plaintiffs and New York Subclass members that they could not reasonably avoid.

534. As a direct and proximate result of Caesars' deceptive and unlawful acts and practices, Plaintiffs and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as

described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

535. Plaintiffs and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

CLAIM FOR RELIEF XV
VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
73 Pa. Cons. Stat. §§ 201-1, *et seq.*
Brought by Pennsylvania Plaintiffs Blair-Smith and Katz on behalf of the Pennsylvania Subclass

536. The Pennsylvania Plaintiffs ("Plaintiffs" for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, re-allege and incorporate by reference Paragraphs 1 through 323 as if fully set forth herein.

537. Plaintiffs and Pennsylvania Subclass Members purchased goods and services from Caesars in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2, for personal, family, and/or household purposes.

538. Caesars engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by Plaintiffs and Pennsylvania Subclass in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including but not limited to the following:

- Misrepresenting material facts pertaining to the sale of its goods and services to the Pennsylvania Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Pennsylvania Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of 73 Pa. Cons. Stat. Ann. §§ 201-3(4)(v), (vii),

(ix), and (xxi);

- Misrepresenting material facts pertaining to the sale of its goods and services to Plaintiffs and Pennsylvania Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Pennsylvania Subclass Members' Personal Information in violation of 73 Pa. Cons. Stat. Ann. §§ 201-3(4) (v), (vii), (ix), and (xxi);
- Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Pennsylvania Subclass Members' Personal Information in violation of in violation of 73 Pa. Cons. Stat. Ann. §§ 201-3(4)(v), (vii), (ix), and (xxi);

539. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of its goods and services by failing to maintain the privacy and security of Plaintiffs' and Pennsylvania Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to:

- Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of its goods and services by failing to disclose the Data Breach to Plaintiffs and Pennsylvania Subclass Members in a timely and accurate manner, in violation of 73 Pa. Cons. Stat. § 2303(a); and
- Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of its goods and services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Pennsylvania Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

540. The above unlawful, unfair, and deceptive acts and practices by Caesars were

immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Pennsylvania Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

541. Caesars knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Pennsylvania Subclass Members' Personal Information and that risk of a data breach or theft was high. Caesars' numerous past data breaches put it on notice that its security and privacy protections were inadequate. Caesars' actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Plaintiffs and Pennsylvania Subclass.

542. As a direct and proximate result of Caesars' unlawful practices, Plaintiffs and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach. Caesars' unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Pennsylvania Subclass Members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

543. Plaintiffs and Pennsylvania Subclass Members seek relief under 73 Pa. Cons. Stat. § 201-9.2, including, but not limited to, injunctive relief, actual damages or statutory damages of $200 per violation (whichever is greater), treble damages, and reasonable attorneys' fees and costs.

/ / /

/ / /

/ / /

CLAIM FOR RELIEF XVI
VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES-CONSUMER PROTECTION ACT
Texas Bus. & Com. Code § 17.41, *et seq.*
Brought by Texas Plaintiff Huddleston on behalf of the Texas Subclass

544. The Texas Plaintiff ("Plaintiff" for purposes of this Count), individually and on behalf of the Texas Subclass, re-alleges and incorporates by reference Paragraphs 1 through 323 as if fully set forth herein.

545. Caesars is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

546. Plaintiff and the Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

547. Caesars advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

548. Caesars engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

- Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;
- Representing that goods or services are of a particular standard, quality or grade, if they are of another; and
- Advertising goods or services with intent not to sell them as advertised; and
- Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

549. Caesars' false, misleading, and deceptive acts and practices include:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the

Data Breach;

- Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;
- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;
- Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and
- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

550. Caesars intended to mislead Plaintiff and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

551. Caesars' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Caesars' data security and ability to protect the confidentiality of consumers' PII.

552. Had Caesars disclosed to Plaintiff and Subclass Members that its data systems were

not secure and, thus, vulnerable to attack, Caesars would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Caesars was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Caesars accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Caesars' misrepresentations and omissions, the truth of which they could not have discovered.

553. Caesars had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and Texas Subclass Members, and Caesars because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Caesars. Caesars' duty to disclose also arose from its:

- Possession of exclusive knowledge regarding the security of the data in its systems;
- Active concealment of the state of its security; and/or
- Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and Texas Subclass Members that contradicted these representations.

554. Caesars engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Caesars engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

555. Consumers, including Plaintiff and Texas Subclass Members, lacked knowledge about deficiencies in Caesars' data security because this information was known exclusively by Caesars. Consumers also lacked the ability, experience, or capacity to secure the PII in Caesars' possession or to fully protect their interests with regard to their data. Plaintiff and Texas Subclass Members lack expertise in information security matters and do not have access to Caesars' systems

in order to evaluate its security controls. Caesars took advantage of its special skill and access to PII to hide its inability to protect the security and confidentiality of Plaintiffs' and Texas Subclass Members' PII.

556. Caesars intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Caesars' conduct is glaring, flagrant, complete, and unmitigated. The Data Breach, which resulted from Caesars' unconscionable business acts and practices, exposed Plaintiff and Texas Subclass Members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented numbers of consumers. Plaintiffs and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

557. Caesars acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass Members' rights. Caesars' numerous past data breaches put it on notice that its security and privacy protections were inadequate.

558. As a direct and proximate result of Caesars' unconscionable and deceptive acts or practices, Plaintiff and Texas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach. Caesars' unconscionable and deceptive acts or practices were a producing cause of Plaintiff's and Texas Subclass Members' injuries, ascertainable losses, economic damages, and non- economic damages, including their mental anguish.

559. Caesars' violations present a continuing risk to Plaintiff and Texas Subclass Members as well as to the general public.

560. Plaintiff has substantially complied with the notice requirements of Tex. Bus. & Com. Code § 17.505. In addition, Caesars received written notice of the factual bases of this cause of action and others when plaintiffs in multiple actions that were filed in multiple jurisdictions served Caesars with complaints in connection with the Data Breach. Those complaints were filed more than 90 days ago, prior to the consolidation of the actions in the United States District Court for the District of Nevada.

561. These actions contained similar factual allegations to those giving rise to this cause of action, and Caesars has therefore had ample opportunity to investigate the basis of this action and pursue settlement discussions.

562. To date, Caesars has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiffs' counsel.

563. Contemporaneous with the filing of this Consolidated Complaint, pursuant to Tex. Bus. & Com. Code Ann. § 17.501, Plaintiff's counsel will send to the Consumer Protection Division a copy of the written notice sent to Caesars.

564. Plaintiff and Texas Subclass Members seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

CLAIM FOR RELIEF XVII
VIOLATION OF THE VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT
Va. Code. Ann. §§ 18.2-186.6, *et seq.*
On behalf of Virginia Plaintiff Lackey on behalf of the Virginia Subclass

565. The Virginia Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, re-allege and incorporate by reference all preceding allegations in Paragraphs 1 through 323 as if fully set forth herein.

566. Caesars is required to accurately notify Plaintiff and Virginia Subclass members following discovery or notification of a breach of its data security system if unencrypted or

unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

567. Caesars is an entity that owns or licenses computerized data that includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(B).

568. Plaintiff's and Virginia Subclass members' Personal Information includes Personal Information as covered under Va. Code Ann. § 18.2-186.6(A).

569. Because Caesars discovered a breach of its security system in which unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Caesars had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

570. By failing to disclose the Data Breach in a timely and accurate manner, Caesars violated Va. Code Ann. § 18.2-186.6(B).

571. As a direct and proximate result of Caesars' violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Virginia Subclass members suffered damages, as described above.

572. Plaintiff and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

CLAIM FOR RELIEF XVIII
VIOLATION OF THE VIRGINIA CONSUMER PROTECTION ACT
Va. Code Ann. §§ 59.1-196, *et seq.*
On behalf of Virginia Plaintiff Lackey on behalf of the Virginia Subclass

573. The Virginia Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, re-allege and incorporate by reference all preceding allegations in Paragraphs 1 through 323 as if fully set forth herein.

574. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

575. Caesars is a "person" as defined by Va. Code Ann. § 59.1-198.

576. Caesars is a "supplier," as defined by Va. Code Ann. § 59.1-198.

577. Caesars engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Caesars advertised, offered, or sold goods or services used primarily for personal, family or household purposes; or relating to an individual's finding or obtaining employment.

578. Caesars engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virginia Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virginia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- Omitting, suppressing, and concealing the material fact that it did not reasonably or

adequately secure Plaintiff and Virginia Subclass members' Personal Information; and

- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

579. Caesars intended to mislead Plaintiff and Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

580. Caesars' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Virginia Subclass members, about the adequacy of Caesars' computer and data security and the quality of the Caesars brand.

581. Had Caesars disclosed to Plaintiff and Virginia Subclass members that its data systems were not secure and, thus, vulnerable to attack, Caesars would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Caesars received, maintained, and compiled Plaintiff's and Virginia Subclass members' Personal Information as part of the services Caesars provided and for which Plaintiff and Virginia Subclass members paid without advising Plaintiff and Virginia Subclass members that Caesars' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Virginia Subclass members' Personal Information. Accordingly, Plaintiff and the Virginia Subclass members acted reasonably in relying on Caesars' misrepresentations and omissions, the truth of which they could not have discovered.

582. Caesars had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virginia Subclass—and Caesars, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Caesars. Caesars' duty to disclose also arose from its:

- Possession of exclusive knowledge regarding the security of the data in its systems;

- Active concealment of the state of its security; and/or
- Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virginia Subclass that contradicted these representations.

583. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

- Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;
- Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and
- Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

584. Caesars acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Virginia Subclass members' rights. Caesars' past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish Caesars for its wrongdoing, and warn or deter others from engaging in similar conduct.

585. As a direct and proximate result of Caesars' deceptive acts or practices, Plaintiffs and Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Caesars as they would not have paid Caesars for goods and services or would have paid less for such goods and services but for Caesars' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

586. Caesars' violations present a continuing risk to Plaintiffs and Virginia Subclass

members as well as to the general public.

587. Plaintiffs and Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated individuals, respectfully request the following relief:

(a) An Order certifying this case as a class action;

(b) An Order appointing Plaintiffs as class representatives;

(c) An Order appointing the undersigned counsel as class counsel;

(d) Injunctive relief requiring Caesars to: (i) strengthen its data security systems and procedures; (ii) submit to future annual audits of those systems by a Court-appointed independent auditor; and (iv) delete PII that Caesars no longer needs for processing services previously provided to Class Members;

(e) An award of nominal damages, compensatory damages, money for significant and reasonable credit monitoring, statutory damages, treble damages, and punitive damages;

(f) An award of Plaintiffs' attorneys' fees and litigation costs; and

(g) Such other and further relief as this Court may deem just and proper.

IX. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury as to all issues so triable.

DATED this 29th day of July, 2024.

Respectfully submitted,

KEMP JONES, LLP

/s/ Michael J. Gayan
Don Springmeyer, Esq. (#1021)
Michael J. Gayan, Esq.(#11135)

3800 Howard Hughes Parkway, 17th Floor
Las Vegas, Nevada 89169

Liaison Counsel

Douglas J. McNamara
Cohen Milstein Sellers & Toll PLLC
1100 New York Ave. NW, 5th Floor
Washington, D.C. 20005

Amy E. Keller
DiCello Levitt LLP
10 North Dearborn Street, Sixth Floor
Chicago, Illinois 60602

Interim Class Counsel

Jeff Ostrow
Kopelowitz Ostrow, P.A.
1 West Las Olas Blvd, 5th Floor
Ft. Lauderdale, Florida 33301

Plaintiff's Steering Committee Chair

James Pizzirusso
Hausfeld LLP
888 16th Street N.W., Suite 300
Washington, D.C. 20006

Gerard Stranch
Stranch, Jennings & Garvey, PLLC
223 Rosa L Parks Ave, Suite #200
Nashville, Tennessee 37203

Gary M. Klinger
Milberg Coleman Bryson Phillips
Grossman, PLLC
227 W. Monroe Street, Suite #2100
Chicago, Illinois 60606

Sabita J. Soneji
Tycko & Zavareei LLP
1970 Broadway, Suite 1070
Oakland, California 94612

Linda P. Nussbaum
Nussbaum Law Group, P.C.
1133 Avenue of the Americas, 31st Floor
New York, New York 10036

Plaintiffs' Steering Committee

CERTIFICATE OF SERVICE

I hereby certify that on this 29th day of July, 2024, a true and correct copy of **CONSOLIDATED CLASS ACTION COMPLAINT** was served via the United States District Court CM/ECF system on all counsel of record who have enrolled in this ECF system.

/s/ Pamela McAfee
An employee of Kemp Jones LLP